US009514446B1

(12) **United States Patent**
Rajkumar et al.

(10) **Patent No.: US 9,514,446 B1**
(45) **Date of Patent: *Dec. 6, 2016**

(54) **REMARKETING CONTENT TO A USER ASSOCIATED WITH MULTIPLE DEVICES**

(71) Applicant: **Google Inc.**, Mountain View, CA (US)

(72) Inventors: **Nareshkumar Rajkumar**, San Jose, CA (US); **Vinod Kumar Ramachandran**, Sunnyvale, CA (US)

(73) Assignee: **Google Inc.**, Mountain View, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 434 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **13/648,651**

(22) Filed: **Oct. 10, 2012**

Related U.S. Application Data

(63) Continuation-in-part of application No. 13/458,124, filed on Apr. 27, 2012, now Pat. No. 8,688,984.

(51) **Int. Cl.**

G06F 15/16	(2006.01)
G06Q 10/10	(2012.01)
H04L 12/58	(2006.01)

(52) **U.S. Cl.**
CPC ***G06Q 10/107*** (2013.01); ***H04L 51/14*** (2013.01)

(58) **Field of Classification Search**
CPC G06F 17/30876; G06F 17/30887; G06F 17/30917; G06F 21/6245; G06F 21/6254; G06F 21/6263
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,408,950	A	4/1995	Porto
5,892,900	A	4/1999	Ginter et al.

(Continued)

FOREIGN PATENT DOCUMENTS

EP	2270741	A1	1/2011
JP	2004070441	A	3/2004

(Continued)

OTHER PUBLICATIONS

Ebbert, J., "Is Audience Buying Possible in Mobile Advertising?," AdExchanger.com, Aug. 3, 2011 [online] [Retrieved on Dec. 2, 2011]; Retrieved from the Internet URL: http://www.adexchanger.com/mobile/audience-buying/; 9 pages.

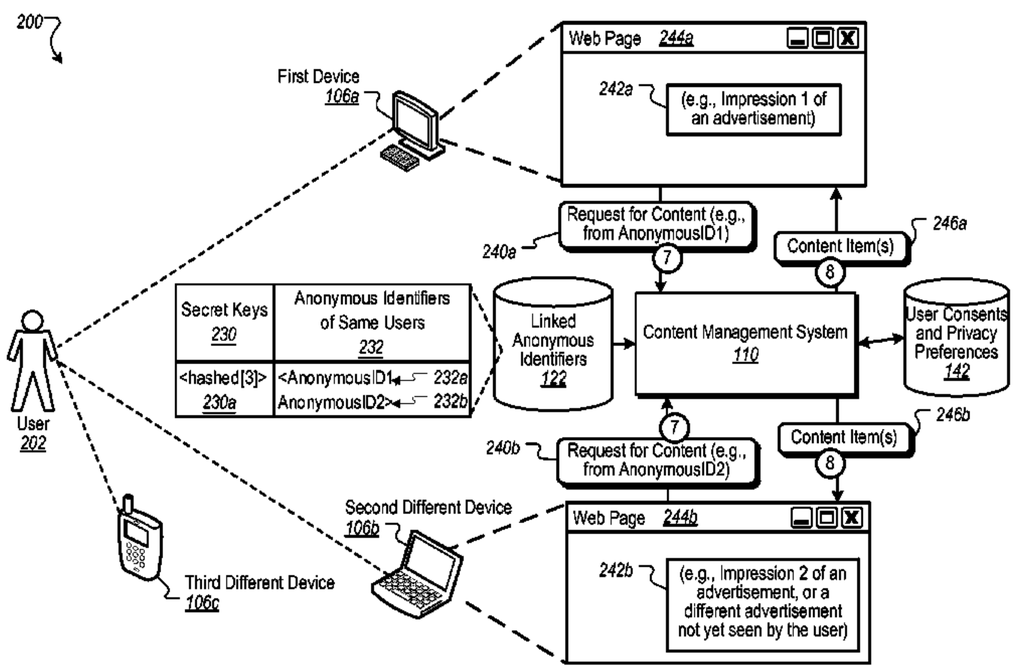
(Continued)

Primary Examiner — Ario Etienne
Assistant Examiner — Blake Rubin
(74) *Attorney, Agent, or Firm* — Fish & Richardson P.C.

(57) **ABSTRACT**

Methods, systems, and apparatus, including computer programs encoded on a computer-readable storage medium, and including a method for selecting content. The method comprises anonymously linking plural identifiers, each associated with a user and specific requesting source. Anonymously linking includes linking at least two different identifiers associated with two different requesting sources used to access content, and linking the two different identifiers using an identifier not including any personally identifiable information. The method further comprises identifying a user list associated with a topic and including plurality of entries, each entry satisfying the topic and having an identifier associated with a requesting source and further including information about a type of requesting source. The method further comprises linking an entry in the user list to other identifiers using the anonymous linking, and selecting content for delivery to a user device associated with an entry in the user list based on the linking.

20 Claims, 12 Drawing Sheets



(56) **References Cited**

U.S. PATENT DOCUMENTS

6,223,178	B1	4/2001	Himmel et al.	
6,324,566	B1	11/2001	Himmel et al.	
6,486,891	B1	11/2002	Rice	
7,308,261	B2	12/2007	Henderson et al.	
7,551,913	B1	6/2009	Chien	
7,711,707	B2	5/2010	Kelley et al.	
7,729,977	B2 *	6/2010	Xiao et al.	705/37
7,861,260	B2	12/2010	Shkedi	
8,041,602	B2	10/2011	Haley et al.	
8,065,185	B2	11/2011	Foladare et al.	
8,107,408	B2	1/2012	Chindapol et al.	
8,140,389	B2 *	3/2012	Altberg et al.	705/14.41
8,271,328	B1	9/2012	Baltz et al.	
8,321,684	B2	11/2012	Mumm et al.	
8,359,274	B2	1/2013	Yoder et al.	
8,423,408	B1	4/2013	Barnes et al.	
8,438,184	B1 *	5/2013	Wang et al.	707/780
8,447,652	B2	5/2013	Kilroy et al.	
8,533,472	B2 *	9/2013	Takasugi	H04L 9/3236 713/168
8,666,812	B1	3/2014	Gandhi	
8,688,984	B2	4/2014	Rajkumar et al.	
8,798,456	B2	8/2014	Skirmont et al.	
8,799,456	B2	8/2014	de Jager et al.	
8,832,319	B2	9/2014	Kessel et al.	
8,862,889	B2	10/2014	Madden	
8,892,685	B1	11/2014	Rajkumar et al.	
8,966,043	B2	2/2015	Rajkumar et al.	
8,978,158	B2	3/2015	Rajkumar et al.	
9,009,258	B2	4/2015	Ramachandran et al.	
9,087,335	B2 *	7/2015	Rane et al.	
2003/0046290	A1	3/2003	Yamada	
2003/0061275	A1	3/2003	Brown et al.	
2003/0061512	A1	3/2003	Flurry et al.	
2003/0149781	A1	8/2003	Yared et al.	
2003/0217687	A1	11/2003	Segall	
2003/0229900	A1 *	12/2003	Reisman	725/87
2004/0068477	A1 *	4/2004	Gilmour et al.	707/1
2004/0088363	A1	5/2004	Doemling et al.	
2004/0122735	A1	6/2004	Meshkin	
2004/0204997	A1	10/2004	Blaser et al.	
2005/0021747	A1	1/2005	Jave	
2005/0044423	A1	2/2005	Mellmer et al.	
2005/0076248	A1	4/2005	Cahill et al.	
2005/0268102	A1	12/2005	Downey	
2005/0278731	A1	12/2005	Cameron et al.	
2006/0020782	A1	1/2006	Kakii	
2006/0036857	A1	2/2006	Hwang	
2006/0080415	A1	4/2006	Tu	
2006/0101287	A1	5/2006	Morten	
2006/0136717	A1	6/2006	Buer et al.	
2007/0124201	A1	5/2007	Hu et al.	
2007/0136305	A1	6/2007	Kelley et al.	
2007/0136306	A1	6/2007	Kelley et al.	
2007/0174614	A1	7/2007	Duane et al.	
2007/0240226	A1	10/2007	Song et al.	
2008/0052775	A1 *	2/2008	Sandhu et al.	726/14
2008/0098039	A1	4/2008	Kruis et al.	
2008/0140476	A1	6/2008	Anand et al.	
2008/0172373	A1	7/2008	Jenson et al.	
2008/0235243	A1	9/2008	Lee et al.	
2008/0243609	A1 *	10/2008	Murto et al.	705/14
2008/0275753	A1	11/2008	Protheroe et al.	
2009/0013051	A1 *	1/2009	Renschler	G06F 17/30867 709/206
2009/0048922	A1	2/2009	Morgenstern et al.	
2009/0077000	A1	3/2009	Begole et al.	
2009/0094642	A1	4/2009	Hobson	
2009/0132813	A1	5/2009	Schibuk	
2009/0150238	A1	6/2009	Marsh et al.	
2009/0157502	A1	6/2009	Cooper et al.	
2009/0164557	A1 *	6/2009	Marlow et al.	709/203
2009/0234708	A1 *	9/2009	Heiser et al.	705/10
2009/0234909	A1	9/2009	Strandell et al.	
2009/0248496	A1 *	10/2009	Hueter et al.	705/10
2009/0298480	A1	12/2009	Khambete et al.	
2009/0300745	A1 *	12/2009	Dispensa	726/7
2009/0307759	A1	12/2009	Schnell et al.	
2009/0320091	A1	12/2009	Torres et al.	
2010/0057843	A1 *	3/2010	Landsman et al.	709/203
2010/0088519	A1	4/2010	Tsuruoka et al.	
2010/0180009	A1 *	7/2010	Callahan	709/217
2010/0186084	A1	7/2010	Hamid	
2010/0199098	A1 *	8/2010	King	713/182
2010/0293049	A1	11/2010	Maher et al.	
2010/0313009	A1 *	12/2010	Combet et al.	713/150
2010/0318432	A1	12/2010	Zinkevich et al.	
2011/0010243	A1	1/2011	Wilburn et al.	
2011/0047032	A1	2/2011	Kumar et al.	
2011/0055556	A1 *	3/2011	Choi et al.	713/156
2011/0110515	A1	5/2011	Tidwell et al.	
2011/0153428	A1	6/2011	Ramer et al.	
2011/0154499	A1	6/2011	Rohan et al.	
2011/0213977	A1	9/2011	Little	
2011/0231478	A1	9/2011	Wheeler et al.	
2011/0251878	A1	10/2011	Subramanian et al.	
2011/0276383	A1 *	11/2011	Heiser et al.	705/14.25
2011/0289314	A1	11/2011	Whitcomb	
2011/0314114	A1	12/2011	Young et al.	
2012/0023547	A1 *	1/2012	Maxson	G06F 21/6245 726/1
2012/0030554	A1	2/2012	Toya	
2012/0054680	A1	3/2012	Moonka et al.	
2012/0060120	A1	3/2012	Aravamudan et al.	
2012/0096088	A1	4/2012	Fahmy	
2012/0096491	A1	4/2012	Shkedi	
2012/0109734	A1 *	5/2012	Fordyce et al.	705/14.25
2012/0124161	A1 *	5/2012	Tidwell	G06F 21/6254 709/217
2012/0158491	A1	6/2012	Goulden et al.	
2012/0167185	A1	6/2012	Menezes et al.	
2012/0253920	A1	10/2012	Yarvis et al.	
2012/0253926	A1	10/2012	Chen et al.	
2012/0321143	A1	12/2012	Krupka et al.	
2012/0323674	A1	12/2012	Simmons et al.	
2012/0323686	A1	12/2012	Burger et al.	
2012/0324027	A1 *	12/2012	Vaynblat	G06Q 50/01 709/206
2012/0331287	A1 *	12/2012	Bowman et al.	713/156
2013/0036434	A1	2/2013	Shkedi et al.	
2013/0055309	A1	2/2013	Dittus	
2013/0110623	A1	5/2013	Kilroy et al.	
2013/0124309	A1 *	5/2013	Traasdahl et al.	705/14.49
2013/0124628	A1 *	5/2013	Weerasinghe	709/204
2013/0159254	A1	6/2013	Chen et al.	
2013/0169434	A1	7/2013	McCown et al.	
2013/0179502	A1	7/2013	Faller et al.	
2013/0238745	A1	9/2013	Ramachandran et al.	
2013/0246527	A1	9/2013	Viera	
2013/0252628	A1	9/2013	Kuehnel	
2013/0254685	A1 *	9/2013	Batraski et al.	715/760
2013/0290503	A1	10/2013	Rajkumar et al.	
2013/0290711	A1	10/2013	Rajkumar et al.	
2013/0291123	A1	10/2013	Rajkumar et al.	
2013/0332987	A1 *	12/2013	Tenneti	G06F 21/10 726/1
2014/0123309	A1 *	5/2014	Jung	G06F 21/6245 726/27
2014/0188766	A1 *	7/2014	Waldman	G06F 17/30994 705/400
2014/0244351	A1 *	8/2014	Symons	705/7.29
2015/0100426	A1 *	4/2015	Hartzell	G06Q 30/0261 705/14.58
2015/0127628	A1	5/2015	Rathod	

FOREIGN PATENT DOCUMENTS

JP	2007102780	A	4/2007
JP	2011-096093	A	5/2011
KR	10-2012-0004054		1/2012

(56) **References Cited**

FOREIGN PATENT DOCUMENTS

WO	WO2007059087 A2	5/2007
WO	WO 2011/109865	9/2011

OTHER PUBLICATIONS

Marshall, J., "Device Fingerprinting Could Be Cookie Killer," ClickZ.com, Mar. 2, 2011 [online] [Retrieved on Dec. 2, 2011]; Retrieved from the Internet URL: http://www.clickz.com/clickz/news/2030243/device-fingerprinting-cookie-killer; 4 pages.
International Search Report in International Application No. PCT/US2013/038461, mailed Sep. 17, 2013, 12 pages.
International Search Report in International Application No. PCT/US2013/038457, mailed Sep. 17, 2013, 10 pages.
International Search Report in International Application No. PCT/US2013/038482, mailed Aug. 12, 2013, 10 pages.
International Search Report and Written Opinion for Application No. PCT/US2013/029384, dated Jun. 17, 2013, 12 pages.

* cited by examiner

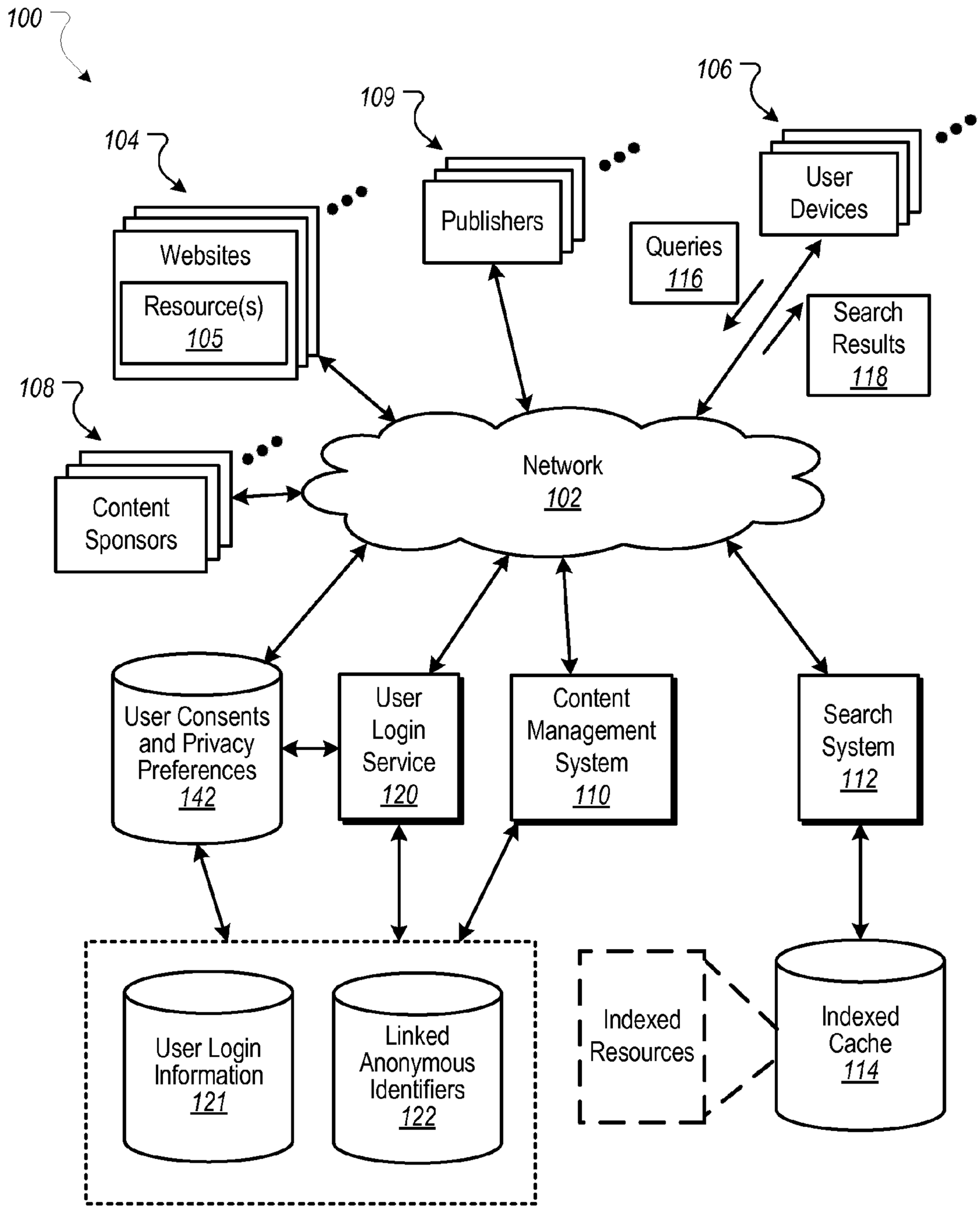

100
104
Websites
Resource(s)
105
108
Content
Sponsors
109
Publishers
106
User
Devices
Queries
116
Search
Results
118
Network
102
User Consents
and Privacy
Preferences
142
User
Login
Service
120
Content
Management
System
110
Search
System
112
User Login
Information
121
Linked
Anonymous
Identifiers
122
Indexed
Resources
Indexed
Cache
114

FIG. 1

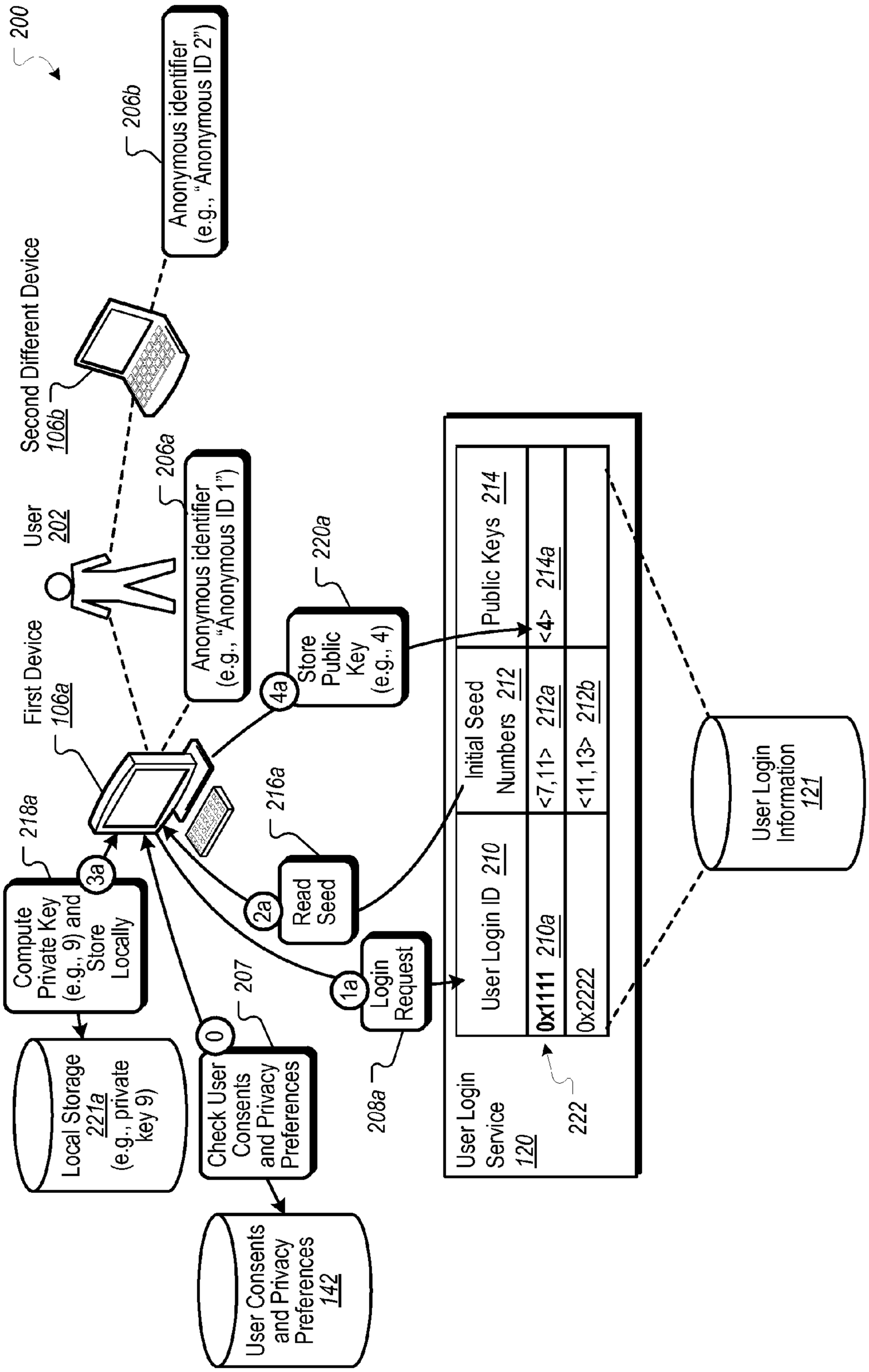

200
206b
Anonymous identifier (e.g., "Anonymous ID 2")
Second Different Device 106b
User 202
206a
Anonymous identifier (e.g., "Anonymous ID 1")
First Device 106a
220a
Store Public Key (e.g., 4)
4a
218a
216a
Compute Private Key (e.g., 9) and Store Locally
3a
Read Seed
2a
Login Request
1a
207
0
Check User Consents and Privacy Preferences
Local Storage 221a (e.g., private key 9)
User Consents and Privacy Preferences 142
208a
User Login ID 210
Initial Seed Numbers 212
Public Keys 214
0x1111 210a
<7,11> 212a
<4> 214a
0x2222
<11,13> 212b
User Login Service 120
222
User Login Information 121

FIG. 2A

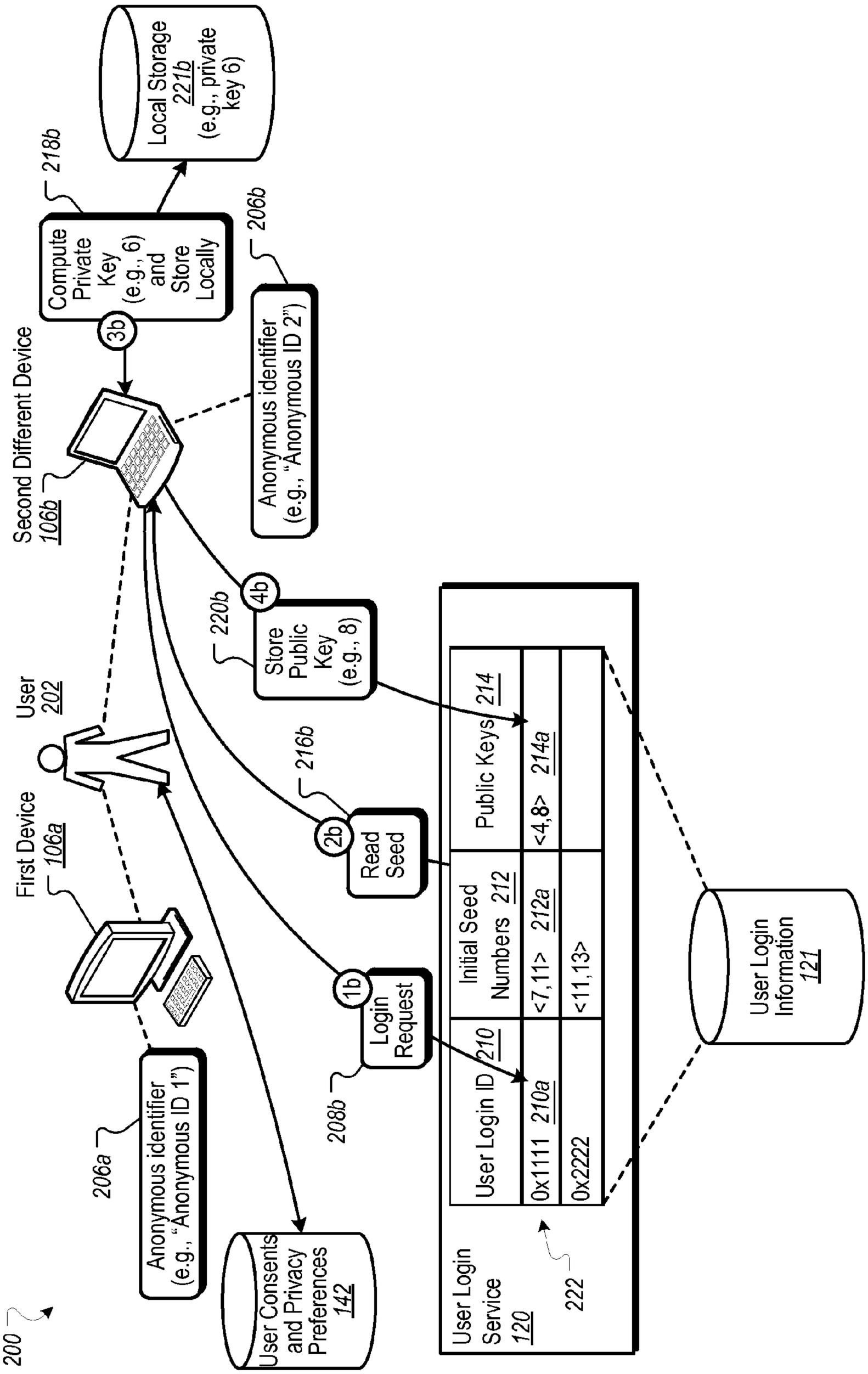

200
First Device 106a
Second Different Device 106b
User 202
Anonymous identifier (e.g., "Anonymous ID 1") 206a
Anonymous identifier (e.g., "Anonymous ID 2") 206b
1b Login Request
208b
2b Read Seed
216b
3b Compute Private Key (e.g., 6) and Store Locally
218b
4b Store Public Key (e.g., 8)
220b
Local Storage 221b (e.g., private key 6)
User Login Service 120
222
User Login ID 210
0x1111 210a
0x2222
Initial Seed Numbers 212
<7,11> 212a
<11,13>
Public Keys 214
<4,8> 214a
User Login Information 121
User Consents and Privacy Preferences 142

FIG. 2B

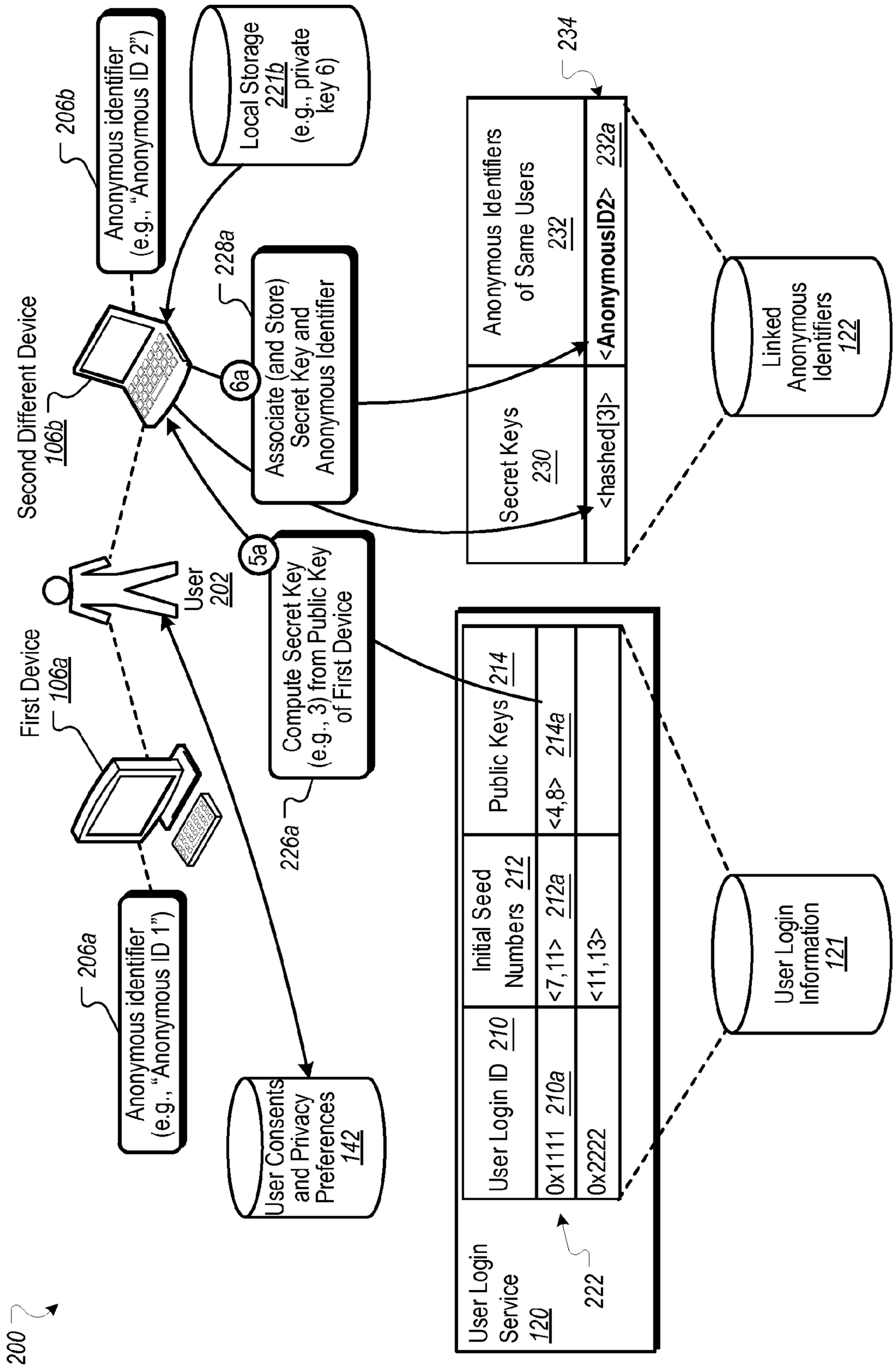

200
First Device 106a
Second Different Device 106b
User 202
206a
Anonymous identifier (e.g., "Anonymous ID 1")
206b
Anonymous identifier (e.g., "Anonymous ID 2")
Local Storage 221b (e.g., private key 6)
228a
Associate (and Store) Secret Key and Anonymous Identifier
6a
5a
Compute Secret Key (e.g., 3) from Public Key of First Device
226a
234
Anonymous Identifiers of Same Users 232
Secret Keys 230
232a
<AnonymousID2>
<hashed[3]>
Linked Anonymous Identifiers 122
User Consents and Privacy Preferences 142
User Login Service 120
222
Initial Seed Numbers 212
Public Keys 214
User Login ID 210
<7,11> 212a
<11,13>
<4,8> 214a
0x1111 210a
0x2222
User Login Information 121

FIG. 2C

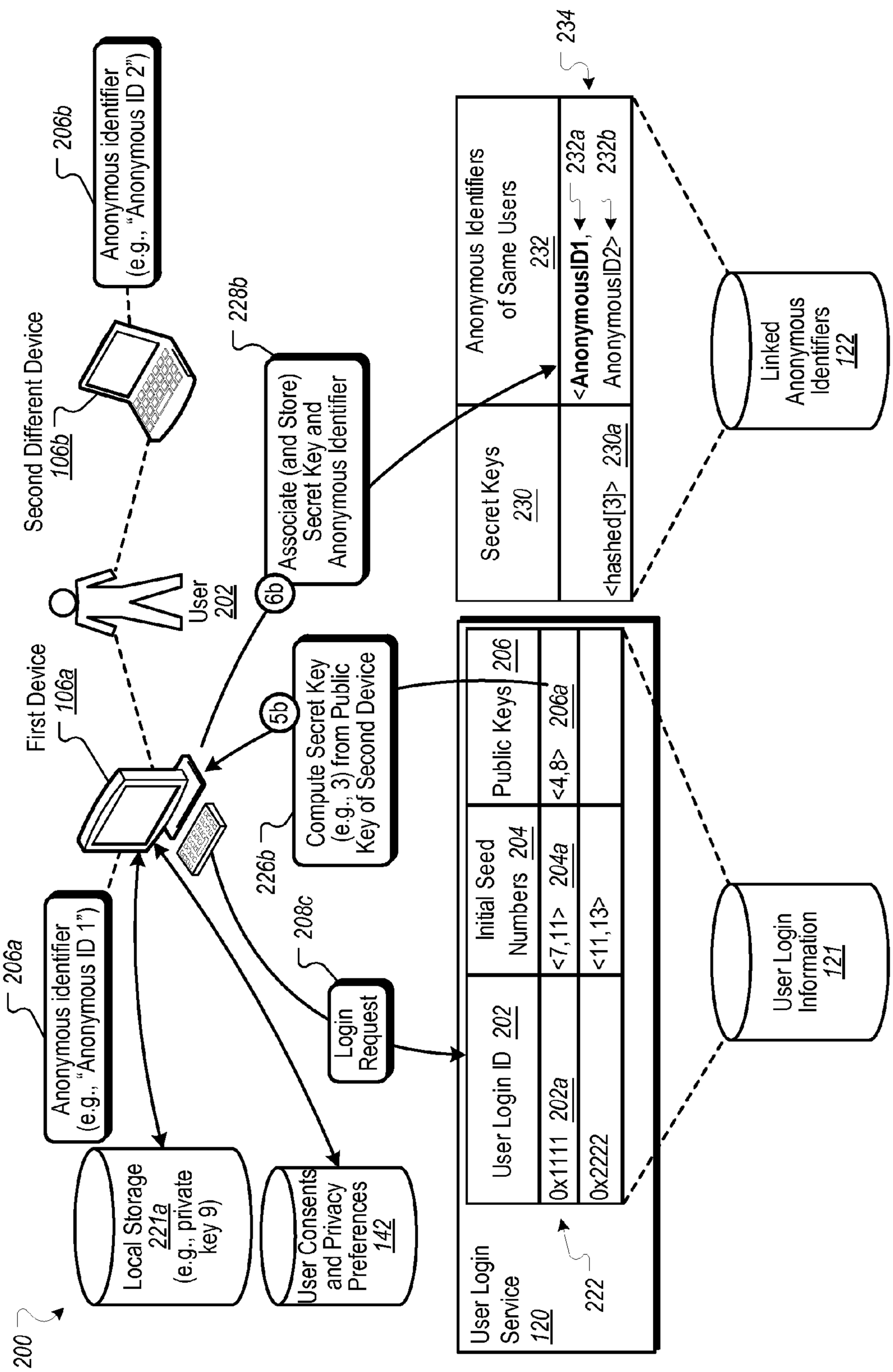

200
First Device 106a
Second Different Device 106b
User 202
Anonymous identifier (e.g., "Anonymous ID 1") 206a
Anonymous identifier (e.g., "Anonymous ID 2") 206b
Local Storage 221a (e.g., private key 9)
User Consents and Privacy Preferences 142
User Login Service 120
222
User Login ID 202
Public Keys 206
Initial Seed Numbers 204
0x1111 202a
0x2222
<4,8> 206a
<7,11> 204a
<11,13>
Login Request 208c
Compute Secret Key (e.g., 3) from Public Key of Second Device 5b
226b
Associate (and Store) Secret Key and Anonymous Identifier 6b
228b
Secret Keys 230
<hashed[3]> 230a
Anonymous Identifiers of Same Users 232
<AnonymousID1>, 232a
<AnonymousID2> 232b
Anonymous
234
Linked Anonymous Identifiers 122
User Login Information 121

FIG. 2D

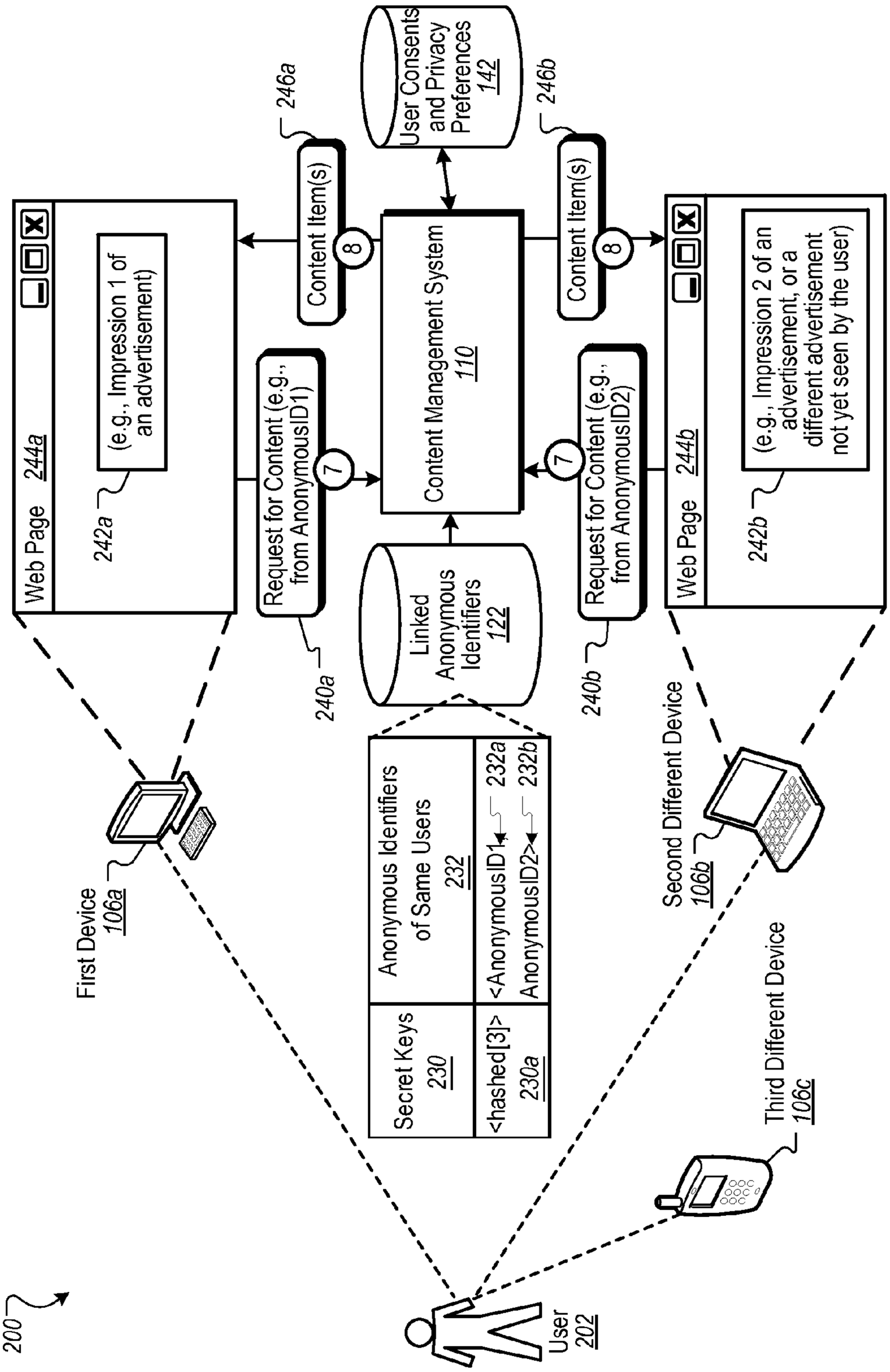

200
User 202
First Device 106a
Second Different Device 106b
Third Different Device 106c
Web Page 244a
242a
(e.g., Impression 1 of an advertisement)
Web Page 244b
242b
(e.g., Impression 2 of an advertisement, or a different advertisement not yet seen by the user)
Request for Content (e.g., from AnonymousID1)
7
240a
Request for Content (e.g., from AnonymousID2)
7
240b
Content Item(s)
8
246a
Content Item(s)
8
246b
Content Management System 110
User Consents and Privacy Preferences 142
Linked Anonymous Identifiers 122
Anonymous Identifiers of Same Users 232
<AnonymousID1> 232a
AnonymousID2> 232b
Secret Keys 230
<hashed[3]> 230a

FIG. 2E

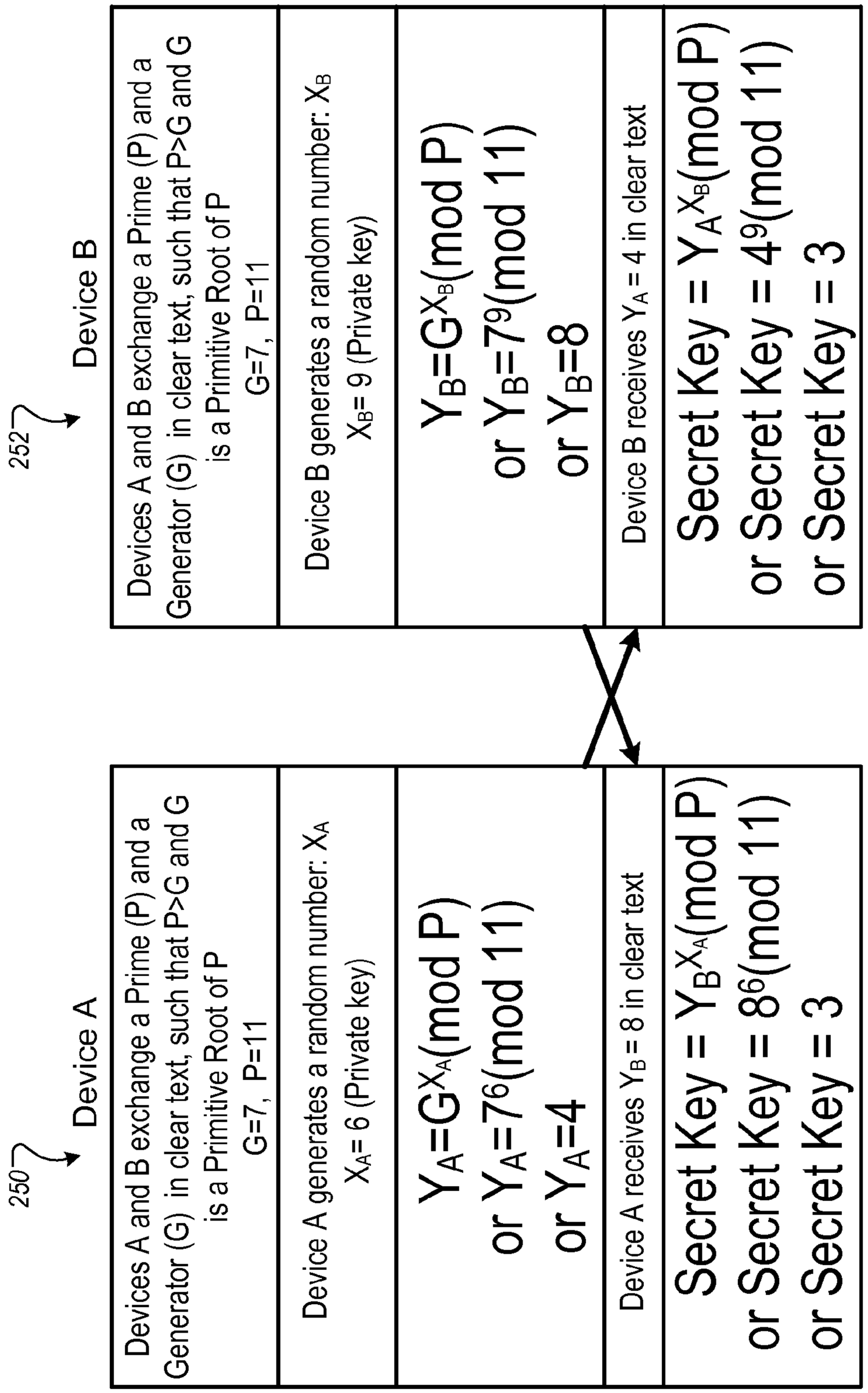

250
Device A
Devices A and B exchange a Prime (P) and a Generator (G) in clear text, such that P>G and G is a Primitive Root of P
G=7, P=11
Device A generates a random number: X_A
X_A= 6 (Private key)
$Y_A=G^{X_A}(\text{mod } P)$
or $Y_A=7^6(\text{mod } 11)$
or $Y_A=4$
Device A receives Y_B = 8 in clear text
Secret Key = $Y_B^{X_A}(\text{mod } P)$
or Secret Key = $8^6(\text{mod } 11)$
or Secret Key = 3
Step 1 254a
Step 2 254b
Step 3 254c
Step 4 254d
Step 5 254e
252
Device B
Devices A and B exchange a Prime (P) and a Generator (G) in clear text, such that P>G and G is a Primitive Root of P
G=7, P=11
Device B generates a random number: X_B
X_B= 9 (Private key)
$Y_B=G^{X_B}(\text{mod } P)$
or $Y_B=7^9(\text{mod } 11)$
or $Y_B=8$
Device B receives Y_A = 4 in clear text
Secret Key = $Y_A^{X_B}(\text{mod } P)$
or Secret Key = $4^9(\text{mod } 11)$
or Secret Key = 3

FIG. 2F

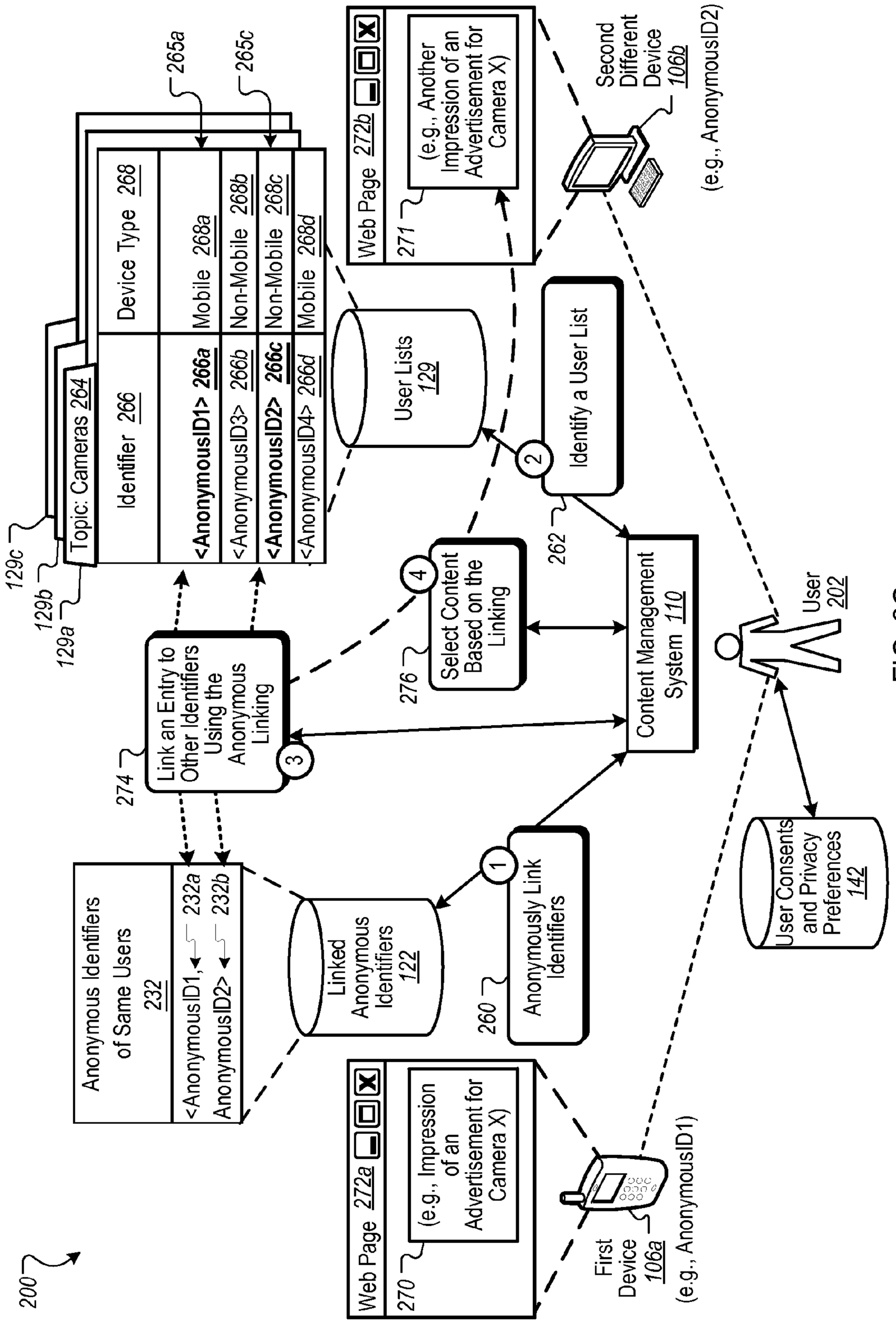

200
Anonymous Identifiers of Same Users 232
<AnonymousID1, 232a
AnonymousID2> 232b
Linked Anonymous Identifiers 122
Anonymously Link Identifiers
260
1
Web Page 272a
(e.g., Impression of an Advertisement for Camera X)
270
First Device 106a
(e.g., AnonymousID1)
User Consents and Privacy Preferences 142
User 202
Content Management System 110
Link an Entry to Other Identifiers Using the Anonymous Linking
274
3
Select Content Based on the Linking
276
4
Identify a User List
262
2
User Lists 129
129c
129b
129a
Topic: Cameras 264
Identifier 266
Device Type 268
<AnonymousID1> 266a
Mobile 268a
<AnonymousID3> 266b
Non-Mobile 268b
<AnonymousID2> 266c
Non-Mobile 268c
<AnonymousID4> 266d
Mobile 268d
265a
265c
Web Page 272b
271
(e.g., Another Impression of an Advertisement for Camera X)
Second Different Device 106b
(e.g., AnonymousID2)

FIG. 2G

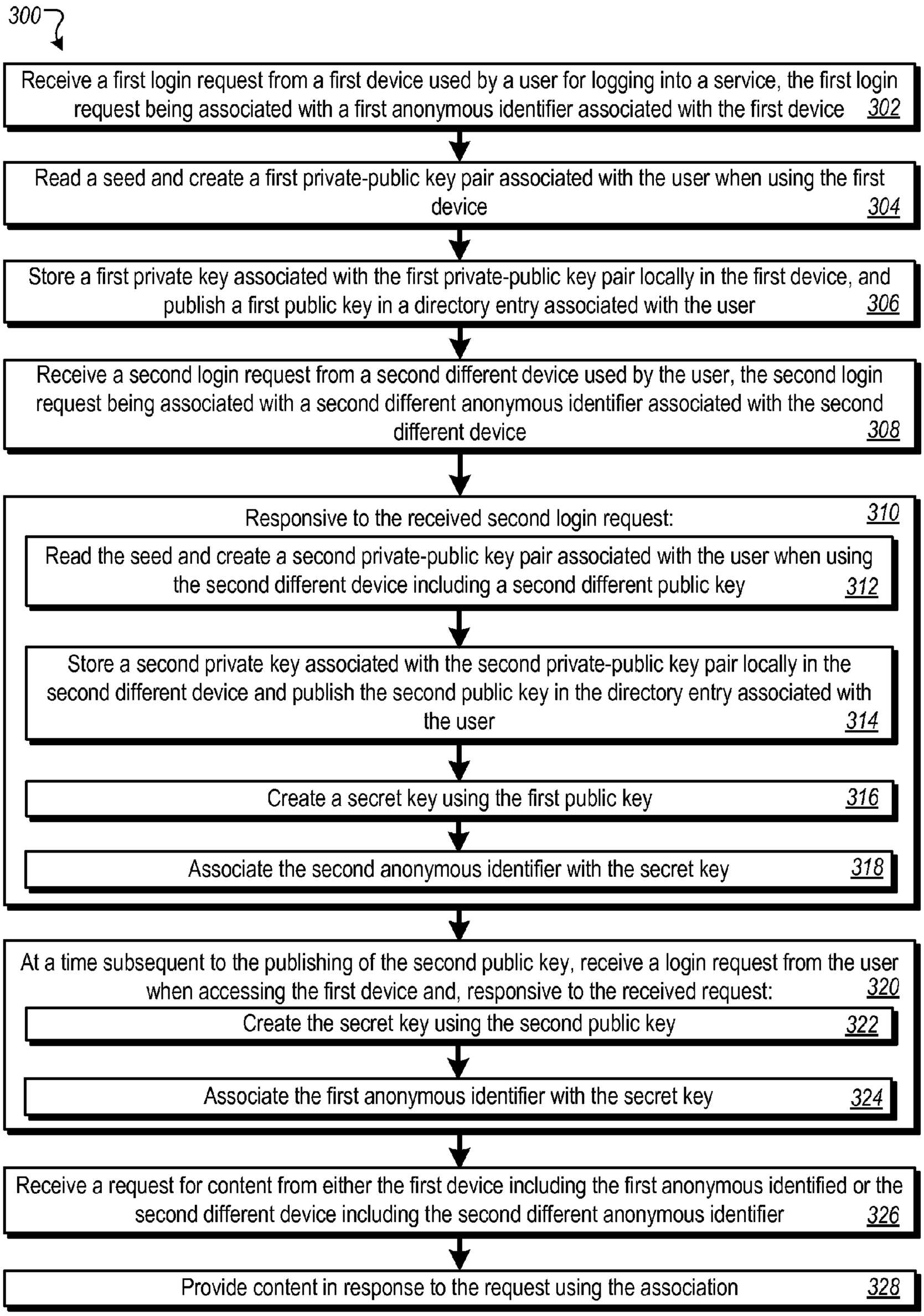

300
Receive a first login request from a first device used by a user for logging into a service, the first login request being associated with a first anonymous identifier associated with the first device 302
Read a seed and create a first private-public key pair associated with the user when using the first device 304
Store a first private key associated with the first private-public key pair locally in the first device, and publish a first public key in a directory entry associated with the user 306
Receive a second login request from a second different device used by the user, the second login request being associated with a second different anonymous identifier associated with the second different device 308
Responsive to the received second login request: 310
Read the seed and create a second private-public key pair associated with the user when using the second different device including a second different public key 312
Store a second private key associated with the second private-public key pair locally in the second different device and publish the second public key in the directory entry associated with the user 314
Create a secret key using the first public key 316
Associate the second anonymous identifier with the secret key 318
At a time subsequent to the publishing of the second public key, receive a login request from the user when accessing the first device and, responsive to the received request: 320
Create the secret key using the second public key 322
Associate the first anonymous identifier with the secret key 324
Receive a request for content from either the first device including the first anonymous identified or the second different device including the second different anonymous identifier 326
Provide content in response to the request using the association 328

FIG. 3A

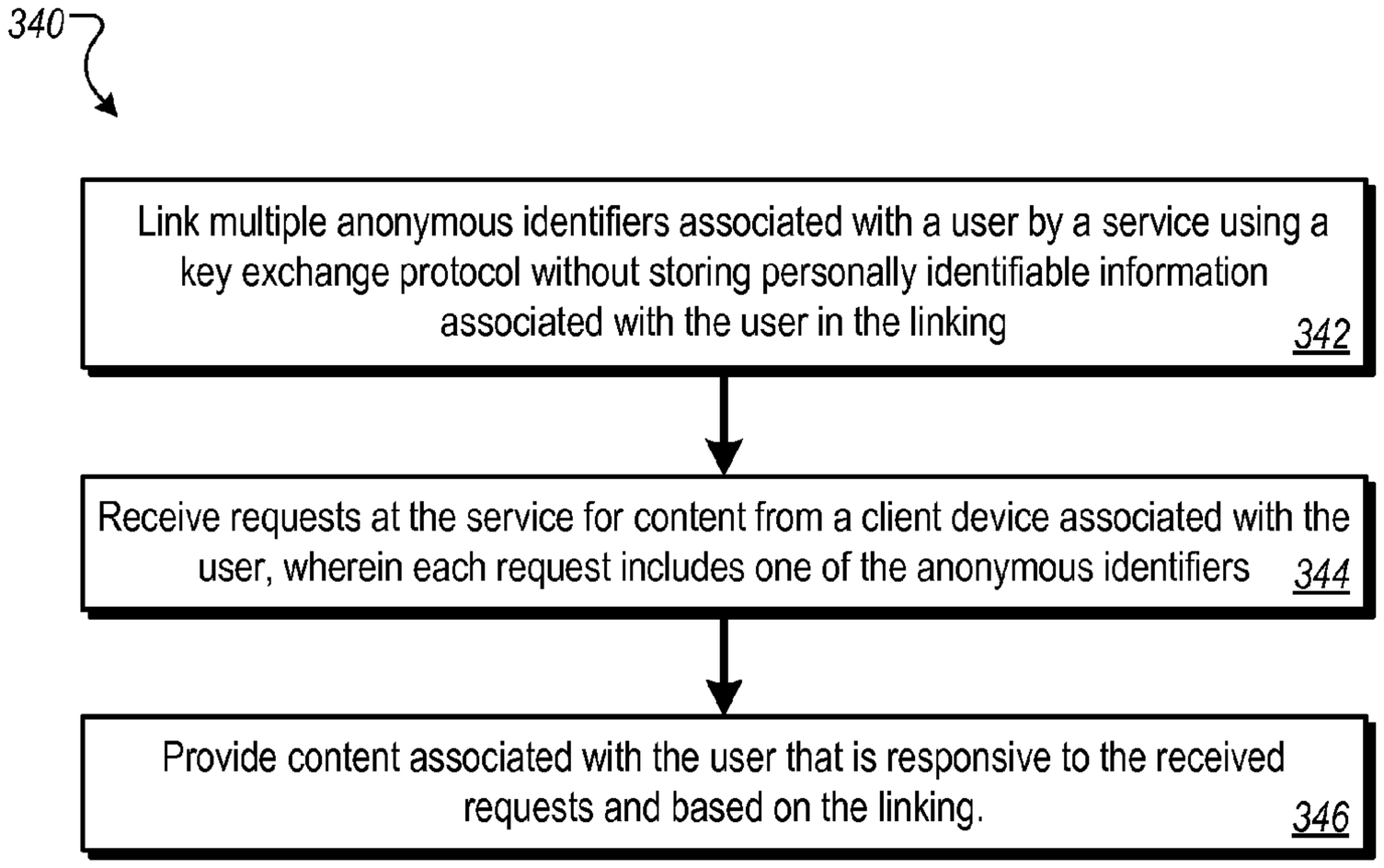

340
Link multiple anonymous identifiers associated with a user by a service using a key exchange protocol without storing personally identifiable information associated with the user in the linking
342
Receive requests at the service for content from a client device associated with the user, wherein each request includes one of the anonymous identifiers
344
Provide content associated with the user that is responsive to the received requests and based on the linking.
346

FIG. 3B

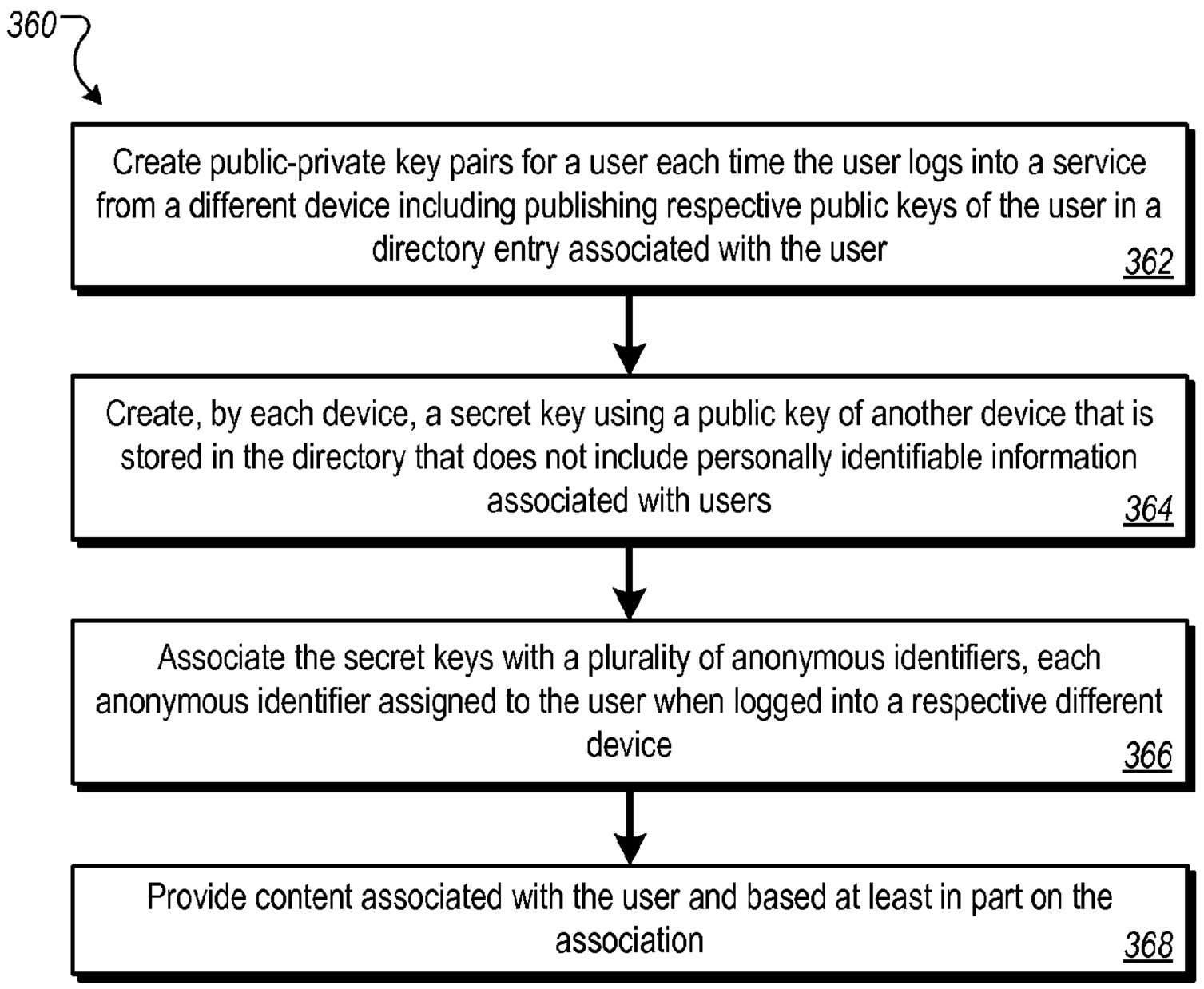

360
Create public-private key pairs for a user each time the user logs into a service from a different device including publishing respective public keys of the user in a directory entry associated with the user
362
Create, by each device, a secret key using a public key of another device that is stored in the directory that does not include personally identifiable information associated with users
364
Associate the secret keys with a plurality of anonymous identifiers, each anonymous identifier assigned to the user when logged into a respective different device
366
Provide content associated with the user and based at least in part on the association
368

FIG. 3C

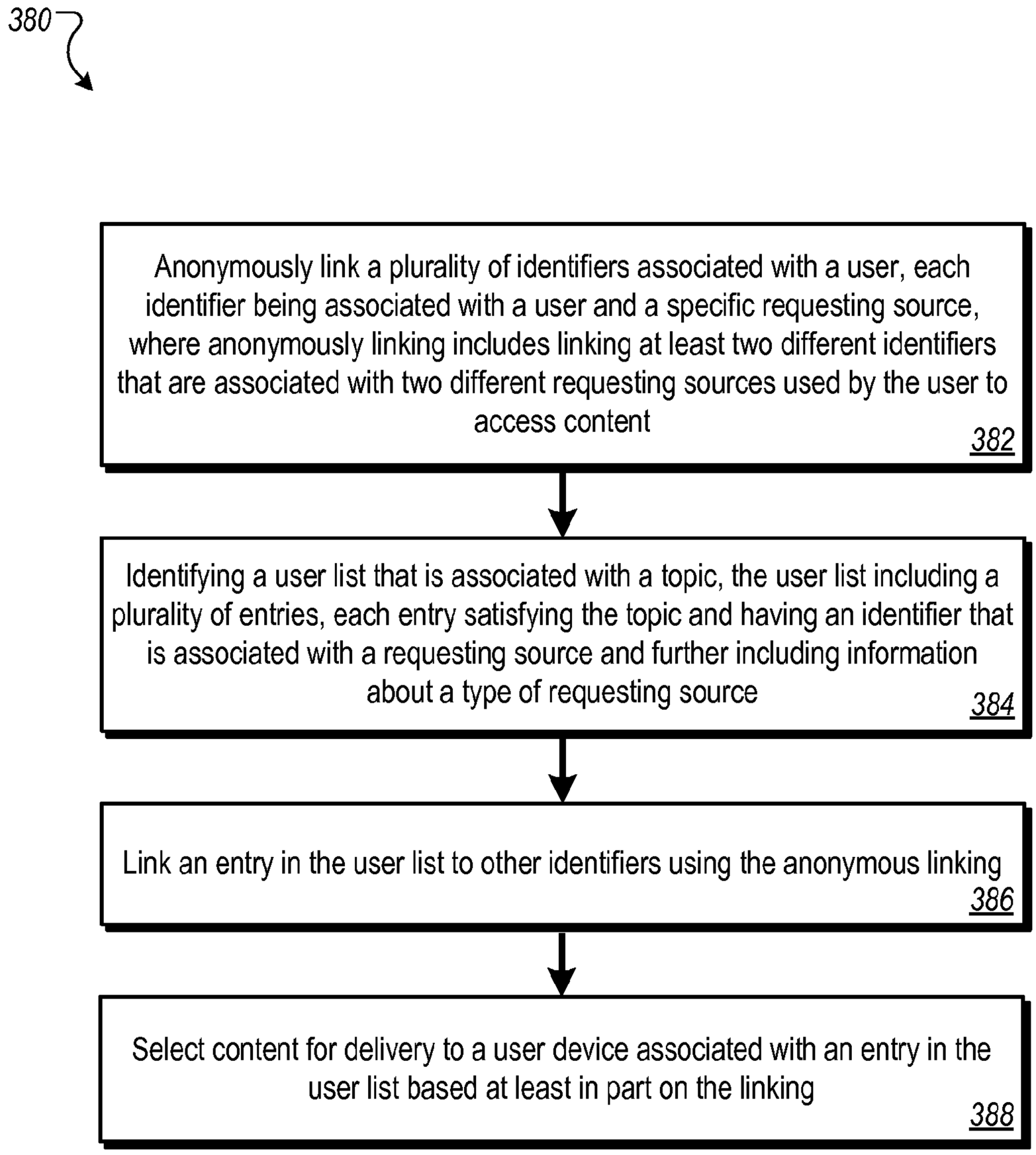

380
Anonymously link a plurality of identifiers associated with a user, each identifier being associated with a user and a specific requesting source, where anonymously linking includes linking at least two different identifiers that are associated with two different requesting sources used by the user to access content
382
Identifying a user list that is associated with a topic, the user list including a plurality of entries, each entry satisfying the topic and having an identifier that is associated with a requesting source and further including information about a type of requesting source
384
Link an entry in the user list to other identifiers using the anonymous linking
386
Select content for delivery to a user device associated with an entry in the user list based at least in part on the linking
388

FIG. 3D

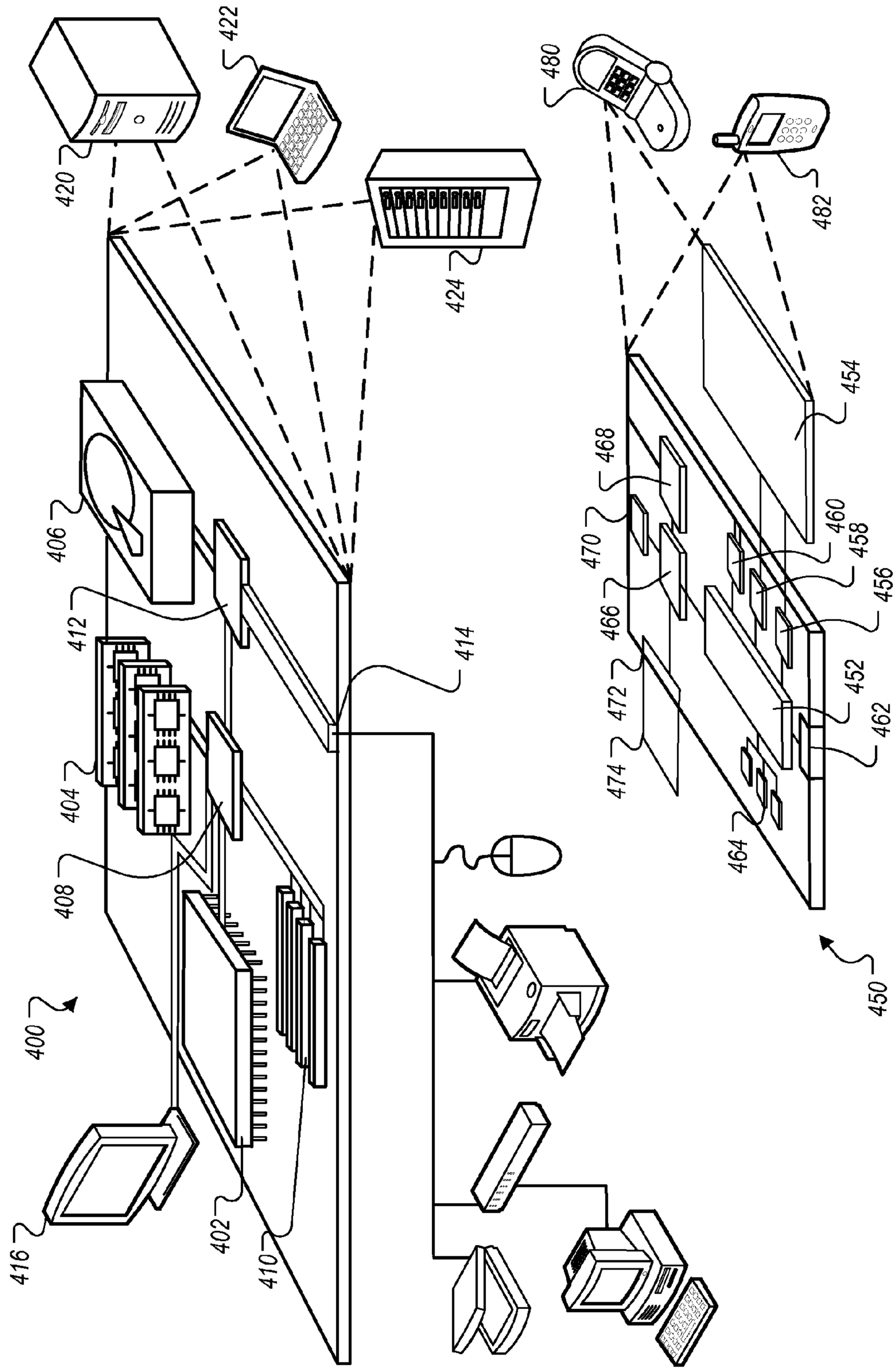

400
402
404
406
408
410
412
414
416
420
422
424
450
452
454
456
458
460
462
464
466
468
470
472
474
480
482

FIG. 4

REMARKETING CONTENT TO A USER ASSOCIATED WITH MULTIPLE DEVICES

CROSS-REFERENCE TO RELATED APPLICATIONS

This application is a continuation-in-part of and claims priority to U.S. application Ser. No. 13/458,124, filed on Apr. 27, 2012, the entire contents of which are hereby incorporated by reference.

BACKGROUND

This specification relates to information presentation.

The Internet provides access to a wide variety of resources. For example, video and/or audio files, as well as web pages for particular subjects or particular news articles, are accessible over the Internet. Access to these resources presents opportunities for other content (e.g., advertisements) to be provided with the resources. For example, a web page can include slots in which content can be presented. These slots can be defined in the web page or defined for presentation with a web page, for example, along with search results.

Content item slots can be allocated to content sponsors as part of a reservation system, or in an auction. For example, content sponsors can provide bids specifying amounts that the sponsors are respectively willing to pay for presentation of their content. In turn, an auction can be run, and the slots can be allocated to sponsors according, among other things, to their bids and/or the relevance of the sponsored content to content presented on a page hosting the slot or a request that is received for the sponsored content. The content can then be provided to the user on a given requesting device.

SUMMARY

In general, one innovative aspect of the subject matter described in this specification can be implemented in methods that include a computer-implemented method for selecting content. The method comprises anonymously linking a plurality of identifiers, each identifier associated with a user and a specific requesting source, wherein anonymously linking includes linking at least two different identifiers that are associated with two different requesting sources used by the user to access content, and wherein anonymously linking includes linking the two different identifiers using an identifier that does not include any personally identifiable information. The method further comprises identifying a user list, the user list associated with a topic and wherein the user list includes a plurality of entries, each entry satisfying the topic and having an identifier that is associated with a requesting source and further including information about a type of requesting source. The method further comprises linking an entry in the user list to other identifiers using the anonymous linking. The method further comprises selecting content for delivery to a user device associated with an entry in the user list based at least in part on the linking.

These and other implementations can each optionally include one or more of the following features. Selecting content can include selecting content for purposes of remarketing content to a user on a second one of multiple requesting sources associated with the user after presentation of content to the user on a first one of the multiple requesting sources associated with the user. Selecting content can be based at least in part on interest profiles for the user on each of the different multiple requesting sources.

The method can further comprise receiving a request to provide a resource to a requesting source and providing to a given device associated with the requesting source an identifier upon access to the resource. The method can further comprise receiving a request for a third party content item where the request includes an identifier and determining when the identifier matches an entry in the user list including determining when the identifier matches an entry in the user list or an identifier associated with an identifier in the user list based at least in part on the anonymous linking. A first identifier included in the user list can be associated with a non-mobile computing device, and a second identifier anonymously linked with the first identifier using the anonymous linking can be associated with a mobile device. A first identifier included in the user list can be associated with a mobile computing device, and a second identifier anonymously linked with the first identifier using the anonymous linking can be associated with a non-mobile device. The method can further comprise crediting a publisher associated with the second identifier. The user list can be used to select subsequent advertisements to be sent to a user device, and the method can further comprise providing an advertisement to a user device based on an identifier that is linked to an entry in the user list. The different requesting sources can be selected from the group comprising: a mobile device including a smart phone, a laptop computer, a tablet, a desktop device, a set-top box, a television, a browser, an application on a mobile device, or a stand-alone application. The method can further comprise identifying a user device associated with linked impressions or interactions from two different requesting sources, wherein an impression has occurred on a first requesting source and an interaction has occurred on a second different requesting source, and identifying content to serve to other users having similar interactions with multiple requesting sources. Identifying content can include identifying content to provide to a user device when a user whose identifier linked by the anonymous linking requests content. Anonymously linking can include linking identifiers using a Diffie-Hellman key exchange protocol. Anonymously linking can include linking identifiers using a secret key derived from a seed that is unique to the user. Selecting content for delivery to the user device associated with the entry in the user list can further be based on a location of the user device. The method can further comprise determining an effective sequence of selecting content for delivery to mobile and non-mobile devices associated with a same user, the effective sequence associated with user behavior of a greater value to a content sponsor than user behavior associated with other different sequences of selecting content for delivery to mobile and non-mobile devices associated with a same user, and selecting content for delivery to a user device associated with an entry in the user list based at least in part on the effective sequence.

Particular implementations may realize none, one or more of the following advantages. For example, content that may be of interest to a user can be provided to the user on any of the user's multiple anonymously-linked devices regardless of which device the user interest associated with the content originated.

The details of one or more implementations of the subject matter described in this specification are set forth in the accompanying drawings and the description below. Other features, aspects, and advantages of the subject matter will become apparent from the description, the drawings, and the claims.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is a block diagram of an example environment for delivering content.

FIGS. 2A through 2E collectively show an example system for providing content to a user who is recognized when using multiple different devices.

FIG. 2F shows example calculations of public, private and secret keys.

FIG. 2G shows an example sequence of events for remarketing content to a user using linked anonymous identifiers of different requesting sources associated with the user.

FIG. 3A is a flowchart of an example process for providing content to a user on any of multiple devices associated with the user.

FIG. 3B is a flowchart of an example process for providing content to a user on any of multiple devices associated with the user.

FIG. 3C is a flowchart of an example process for providing content to a user on any of multiple devices using public-private keys.

FIG. 3D is a flowchart of an example process for remarketing content to a user using linked anonymous identifiers of different requesting sources associated with the user.

FIG. 4 is a block diagram of an example computer system that can be used to implement the methods, systems and processes described in this disclosure.

Like reference numbers and designations in the various drawings indicate like elements.

DETAILED DESCRIPTION

This document describes methods, processes and systems for remarketing content to a user having or being associated with multiple requesting sources (e.g., different devices, applications, etc.), without storing personally identifiable information associated with the user to facilitate content selection. For example, if a user visits a web page associated with cameras using a mobile device (e.g., smart phone, tablet, etc.), the same user can be provided with camera-related content on a non-mobile device (e.g., a personal computer) that is linked to the user's mobile device. Doing so, for example, can satisfy content selection criteria that content sponsors establish for remarketing content, e.g., to provide the same or similar content to a user who has been provided the content before on a different device. Remarketing content to any of a user's different requesting sources can be accomplished, for example, by linking anonymous identifiers associated with the user's different requesting sources, e.g., using a Diffie-Hellman key exchange protocol or in some other way.

In some implementations, the selection of content can be based on user profiles. For example, a user profile that is associated with a user's mobile device may indicate that the user is interested in cameras. At the same time, a user profile that is associated with the user's non-mobile device (e.g., a personal computer (PC)) may not include an indication that the user is interested in cameras. Using information about the user's linked requesting sources, for example, camera-related content can be provided to the user's PC based, at least in part, on the user's camera interest identified in the user profile associated with the user's mobile device.

In some implementations, a more comprehensive interest profile, for remarketing purposes, can be created for a user. For example, the more comprehensive interest profile can be a union of all the user's interest profiles, e.g., for mobile devices and devices at home and at work. As a result, content that is of interest to a user can be provided to any of the user's requesting sources at any time.

Some implementations can allow a user to specify user consents and privacy preferences associated with remarketing based on anonymously linked identifiers corresponding to the user's various requesting sources. For example, a user (e.g., an attorney) can specify that devices should not be linked or that certain topics (e.g., law-related) are not to be used for remarketing. Examples include "Don't remarket law-related content" and "Don't remarket sports-related content to my computer at work." In some implementations, users can remove one or more requesting sources from a set being used in remarketing, or users may choose to disable remarketing on all requesting resources. Some implementations can allow a user to limit remarketing during certain hours of the day. Other options related to consents and privacy preferences can be available.

Different ways can be used to anonymously link a user's different requesting sources. Example requesting sources include a mobile device including a smart phone, a laptop computer, a tablet, a desktop device, a set-top box, a television, a browser, an application on a mobile device, or a stand-alone application. In one example of linking such requesting sources, when a user logs onto a user service from a first device (e.g., the user's home PC), a public key-private key pair can be determined and the public key can be published. The public key can be associated with the user's first device and stored by the user service. The private key can be stored locally. Subsequently, when the user logs into the service from a second different device, the second different device can also determine a public-private key pair. Each device can subsequently compute a secret key using the device's own private key and the other device's published public key. The secret key can be stored in combination with anonymous identifiers of each device, thus creating a linking or association between the sources/devices. The association can be used, for example, in remarketing content for delivery to a user on one of the sources.

In some implementations, the anonymous identifiers can be cookies, browser cookies, device identifiers, or other identifiers that are associated with each device. As a result, the mapping can identify all of the devices associated with the user without storing personally identifiable information (PII) associated with the user. When content is subsequently provided to the user on any of the devices, information included in the mapping can be used to assist in selecting relevant content to be provided to the user. The selection of relevant content can include decisions regarding how content is delivered to the user, such as and including, limitations on when or how content is delivered. For example, the number of impressions of an advertisement can be limited to a fixed number of impressions per user per time period regardless of how many devices the user uses.

In some implementations, anonymous identifiers can be associated with different browsers or other applications on the same device. For example, the techniques described in this disclosure can be used to link two or more identifiers of applications that may have different cookie spaces on the same device, or applications on different devices, or a combination of both.

In some implementations, linking anonymous identifiers can be used in handshaking among mobile applications or a combination of mobile applications, browsers and other applications. For example, mobile applications may each have their own cookie space even on the same device which can prevent handshaking with other applications. Each mobile application can use the techniques described herein to generate, for example, a private key and a public key, publish the public key, access public keys of other mobile applications (or associated with other devices), and compute

secret keys using their own private keys and the public keys of other mobile applications (or associated with other devices).

In some implementations, users may be provided with an opportunity to enable/disable programs or features that allow the user to be discovered across multiple devices and/or to be provided content based on the discovery. For example, the user can enable/disable programs or features related to remarketing, as described above.

In some implementations, the mapping process (e.g., mapping of devices associated with a user) can be repeated periodically to ensure that the anonymous identifiers (e.g., cookies) are not stale, thus keeping session history information for the user up-to-date. For example, cookies on a computer can expire over time, or a user can clear a cookie, resulting in setting a new cookie. Repeating the cookie-mapping process periodically can ensure that the current set of cookies belonging to the user are correctly mapped. While reference is made to cookies, other forms of anonymous identifiers that include or have been derived from a seed can be used.

In some implementations, user session history information can be stored anonymously. For example, the session history information can include a user's browsing history, the times that the user has seen a particular advertisement, and other session history information. The information can be stored in association with the anonymous identifiers described herein. In some implementations, session history information associated with the user's session on a first device can be stored in a table that includes the anonymous identifier associated with the first device. The same table can also be used to store the same user's session history information for the user's session on a second device. In some implementations, a separate or the same table can be used to store associations among the anonymous identifiers. In some implementations, anonymous identifiers, the associations (e g, linking to the secret key), and the session data all can be stored, for example, without any corresponding personally identifiable information for a given user.

As will be described in further detail below, subsequent to the storage of the association and session history information, a request for content (e.g., an advertisement) can be sent from any of the devices associated with that user (the request including an anonymous identifier associated with a given device). In some implementations, the session history information stored in the tables can be used in determining, for example, advertisements that may be of interest to the user responsive to the received request. The determination can include inferences for the user based on the user's stored session history information. In some implementations, the session history information for the user can be aggregated, e.g., by joining tables using the anonymous identifiers. For example, a request for content can be received, and the request can include an anonymous identifier associated with a user's desktop device. The received anonymous identifier can be used to look up the user's other anonymous identifiers (e.g., for mobile and other devices of the user). The retrieved set of anonymous identifiers can be used to access session history information in the other tables (e.g., user browsing history). In some implementations, all of the session history information can be joined together for the respective devices producing aggregated information. In some implementations, the aggregated session history information can be provided to a content management system in order to determine and select eligible content for delivery to the user responsive to the received request. For example, because the session history information can include the number of times that the user has seen a particular advertisement, the content management system can help to avoid selecting an advertisement for the user which has already been presented a predetermined number of times.

In some implementations, aggregating the information can occur on demand, e.g., in real time after a request for content occurs. For example, the user's session history information, stored individually by anonymous identifier in the various tables, can be joined in quasi real time. Aggregating the information in real time can solve issues, for example, related to whether the user has consented to being provided content based on the devices used by the user. For example, session history information for a device for which the user has not consented will not be aggregated with other session history information. In some implementations, the information for a user can be aggregated and stored in advance of any requests for content. For example, all of the user session history information can be stored in a third table, e.g., that includes all of the user session history information across all of the user's devices.

FIG. **1** is a block diagram of an example environment **100** for delivering content. The example environment **100** includes a content management system **110** for selecting and providing content in response to requests for content. The example environment **100** includes a network **102**, such as a local area network (LAN), a wide area network (WAN), the Internet, or a combination thereof. The network **102** connects websites **104**, user devices **106**, content sponsors **108** (e.g., advertisers), publishers **109**, and the content management system **110**. The example environment **100** may include many thousands of websites **104**, user devices **106**, content sponsors **108** and publishers **109**.

In some implementations, the example environment **100** further includes a user login service **120** that can provide, for any particular user, access to the user's Web services, e-mail, social networks, business applications or other resources. For example, the user login service **120** can receive login requests from the user, such as through a Web browser or other application running on any device associated with the user. The login request can include, for example, the user's login ID (e.g., a unique identifier, an email address, a phone number, or any other identifier for the user that can be used for verifying the user at login). The user login service **120** can also maintain information related to the devices on which the user is currently logged on, or has been logged into recently. The information can include, for example, a mapping of anonymous identifiers for the devices with a session key that does not contain personally identifiable information associated with the user. In some implementations, the mapping can be stored, for each user, in a data store of linked anonymous identifiers **122**, or in some data structure.

In some implementations, the user login information **121** or some other data store can store user login IDs, public keys and initial seeds. For example, the information can be used by a second device used by a user to access the public key published by a first device used by the same user. Similarly, the user's first device can access the public key published by the second device. At the same time, seed values can be read from the user login information **121** by any of the user's devices and used to determine a secret key.

A data store of user consents and privacy preferences **142** can include information that the user has provided regarding if and how information about the user's different devices can be used. For example, users can use one or more user preferences web page that may be part of (or separate from) the user login service **120**. In some implementations, users

can set a preference that says, "Do not link my different devices," or selectively identify which devices are allowed (or not allowed) to be linked. Then, before any operation is performed that may link the anonymous identifiers of the user's different devices, the user's consents and privacy preferences can be checked, and the linking will be performed only if allowed by the user. In some implementations, the user may specify settings that prohibit providing content based on the linking. For example, while the user may allow his smart phone and PC to be linked, the user may decide that no content (e.g., advertisements) should be provided based on the linking.

A website **104** includes one or more resources **105** associated with a domain name and hosted by one or more servers. An example website is a collection of web pages formatted in hypertext markup language (HTML) that can contain text, images, multimedia content, and programming elements, such as scripts. Each website **104** can be maintained by a content publisher, which is an entity that controls, manages and/or owns the website **104**.

A resource **105** can be any data that can be provided over the network **102**. A resource **105** can be identified by a resource address that is associated with the resource **105**. Resources include HTML pages, word processing documents, portable document format (PDF) documents, images, video, and news feed sources, to name only a few. The resources can include content, such as words, phrases, images, video and sounds, that may include embedded information (such as meta-information hyperlinks) and/or embedded instructions (such as JavaScript scripts).

A user device **106** is an electronic device that is under control of a user and is capable of requesting and receiving resources over the network **102**. Example user devices **106** include personal computers (PCs), televisions with one or more processors embedded therein or coupled thereto, set-top boxes, mobile communication devices (e.g., smartphones), tablet computers and other devices that can send and receive data over the network **102**. A user device **106** typically includes one or more user applications, such as a web browser, to facilitate the sending and receiving of data over the network **102**.

A user device **106** can request resources **105** from a website **104**. In turn, data representing the resource **105** can be provided to the user device **106** for presentation by the user device **106**. The data representing the resource **105** can also include data specifying a portion of the resource or a portion of a user display, such as a presentation location of a pop-up window or a slot of a third-party content site or web page, in which content can be presented. These specified portions of the resource or user display are referred to as slots (e.g., ad slots).

To facilitate searching of these resources, the environment **100** can include a search system **112** that identifies the resources by crawling and indexing the resources provided by the content publishers on the websites **104**. Data about the resources can be indexed based on the resource to which the data corresponds. The indexed and, optionally, cached copies of the resources can be stored in an indexed cache **114**.

User devices **106** can submit search queries **116** to the search system **112** over the network **102**. In response, the search system **112** accesses the indexed cache **114** to identify resources that are relevant to the search query **116**. The search system **112** identifies the resources in the form of search results **118** and returns the search results **118** to the user devices **106** in search results pages. A search result **118** can be data generated by the search system **112** that identifies a resource that is responsive to a particular search query, and includes a link to the resource. In some implementations, the search results **118** include the content itself, such as a map, or an answer, such as in response to a query for a store's products, phone number, address or hours of operation. In some implementations, the content management system **110** can generate search results **118** using information (e.g., identified resources) received from the search system **112**. An example search result **118** can include a web page title, a snippet of text or a portion of an image extracted from the web page, and the URL of the web page. Search results pages can also include one or more slots in which other content items (e.g., ads) can be presented. In some implementations, slots on search results pages or other web pages can include content slots for content items that have been provided as part of a reservation process. In a reservation process, a publisher and a content item sponsor enter into an agreement where the publisher agrees to publish a given content item (or campaign) in accordance with a schedule (e.g., provide **1000** impressions by date X) or other publication criteria. In some implementations, content items that are selected to fill the requests for content slots can be selected based, at least in part, on priorities associated with a reservation process (e.g., based on urgency to fulfill a reservation).

When a resource **105**, search results **118** and/or other content are requested by a user device **106**, the content management system **110** receives a request for content. The request for content can include characteristics of the slots that are defined for the requested resource or search results page, and can be provided to the content management system **110**.

For example, a reference (e.g., URL) to the resource for which the slot is defined, a size of the slot, and/or media types that are available for presentation in the slot can be provided to the content management system **110**. Similarly, keywords associated with a requested resource ("resource keywords") or a search query **116** for which search results are requested can also be provided to the content management system **110** to facilitate identification of content that is relevant to the resource or search query **116**.

Based at least in part on data included in the request, the content management system **110** can select content that is eligible to be provided in response to the request ("eligible content items"). For example, eligible content items can include eligible ads having characteristics matching the characteristics of ad slots and that are identified as relevant to specified resource keywords or search queries **116**. In some implementations, the selection of the eligible content items can further depend on user signals, such as demographic signals and behavioral signals. Other information, such as user identifier information that is associated with the mappings described above, can be used and/or evaluated when selecting eligible content.

The content management system **110** can select from the eligible content items that are to be provided for presentation in slots of a resource or search results page based at least in part on results of an auction (or by some other selection process). For example, for the eligible content items, the content management system **110** can receive offers from content sponsors **108** and allocate the slots, based at least in part on the received offers (e.g., based on the highest bidders at the conclusion of the auction or based on other criteria, such as those related to satisfying open reservations). The offers represent the amounts that the content sponsors are willing to pay for presentation (or selection) of their content with a resource or search results page. For example, an offer

can specify an amount that a content sponsor is willing to pay for each 1000 impressions (i.e., presentations) of the content item, referred to as a CPM bid. Alternatively, the offer can specify an amount that the content sponsor is willing to pay (e.g., a cost per engagement) for a selection (i.e., a click-through) of the content item or a conversion following selection of the content item. For example, the selected content item can be determined based on the offers alone, or based on the offers of each content sponsor being multiplied by one or more factors, such as quality scores derived from content performance, landing page scores, and/or other factors.

A conversion can be said to occur when a user performs a particular transaction or action related to a content item provided with a resource or search results page. What constitutes a conversion may vary from case-to-case and can be determined in a variety of ways. For example, a conversion may occur when a user clicks on a content item (e.g., an ad), is referred to a web page, and consummates a purchase there before leaving that web page. A conversion can also be defined by a content provider to be any measurable or observable user action, such as downloading a white paper, navigating to at least a given depth of a website, viewing at least a certain number of web pages, spending at least a predetermined amount of time on a web site or web page, registering on a website, experiencing media, or performing a social action regarding a content item (e.g., an ad), such as republishing or sharing the content item. Other actions that constitute a conversion can also be used.

In some implementations, the likelihood that a conversion will occur can be improved, such as by recognizing a user when the user has accessed resources using multiple devices. For example, if it is known that a content item (e.g., an advertisement) has already been seen by a user on a first device (e.g., the user's home PC), then a determination can be made (e.g., through parameters) whether or not to provide the same content item to the same user on a different device (e.g., the user's smartphone). This can increase the likelihood of a conversion, for example, by either repeating impressions of an advertisement or avoiding subsequent impressions, depending on how multiple impressions for the advertisement to the same user are predicted to lead to a conversion in either case.

For situations in which the systems discussed here collect personal information about users, or may make use of personal information, the users may be provided with an opportunity to control whether programs or features collect personal information (e.g., information about a user's social network, social actions or activities, profession, a user's preferences, or a user's current location), or to control whether and/or how to receive content from the content server that may be more relevant to the user. In addition, certain data may be anonymized in one or more ways before it is stored or used, so that personally identifiable information is removed. For example, a user's identity may be anonymized so that no personally identifiable information can be determined for the user, or a user's geographic location may be generalized where location information is obtained (such as to a city, ZIP code, or state level), so that a particular location of a user cannot be determined. Thus, the user may have control over how information is collected about him or her and used by a content server.

FIGS. **2**A-**2**E collectively show an example system **200** for providing content to a user who is recognized when using multiple different devices. In some implementations, recognition of the user across different devices can be achieved by linking anonymous identifiers of the user's multiple different devices. As an example, an anonymous identifier **206***a* of a first device **106***a* (e.g., a desktop computer of a user **202**) can be linked to an anonymous identifier **206***b* of a second different device **106***b* (e.g., a laptop computer of the user **202**). In some implementations, the system **200** can be part of the environment **100** that is described above with reference to FIG. **1**. An example sequence of events (e.g., with numbered steps **0** and **1***a* through **8**) follows for associating the anonymous identifiers **206***a* and **206***b* and providing content based on the association. However, other sequences can also be used to link devices **106***a*, **106***b* and additional devices **106** associated with the user **202**. In some implementations, the devices **106***a*, **106***b* and additional devices **106** can be linked using associations stored in the linked anonymous identifiers **122**. The associations can be stored, for example, without storing any personally identifiable information for the user **202**.

Before any linking occurs using the anonymous identifiers associated with a user's different devices, e.g., at step **0**, the user login service **120** (or the content management system **110**) can check **107** the user's consents and privacy preferences **142** to check the user's consents regarding linking. For example, if the user has specified not to allow the user's devices to be linked (or use information thereof), then steps **2***a* though **6***b* will not occur, and the content provided in step **8** may be different.

In some implementations, a first step **1***a* (e.g., as allowed by the user) of the sequence of steps can occur, for example, when the user **202** logs into the first device **106***a* (e.g., the user's desktop computer) using a login service (not shown in FIGS. **2**A-**2**D). For example, the login service or some other component can receive a login request **208***a* from the first device **106***a*. The login request **208***a* can be associated with the anonymous identifier **206***a* (e.g., a cookie or device identifier) associated with the first device **106***a*. In some implementations, the login request **208***a* and/or other login requests can be requests to log into a social service.

In some implementations, the user login information **121** can store user login IDs **210**, seeds **212** and public keys **214** associated with multiple users. The user login information **121**, for example, can serve as a directory that includes one or more entries, each entry indexed by an identifier associated with a given user (e.g., user login identifier, email address, or some other identifier). For example, when the user **202** logs into the device **106***a* using the login service, information stored for the user in the user login information **121** can include a login ID **210***a*, a seed **212***a* (e.g., a generator-prime pair, such as 7, 11, that is usable by all of the user's devices), and, as will be discussed in further detail below, a public key **214**. At the current stage of the sequence of steps, the public key **214** has not yet been determined for the current user. In some implementations, seeds **212** can vary by user, e.g., the seed **212***b* (e.g., generator-prime pair **7**, **13**) for a second user can be different from the seed **212***a*.

At step **2***a*, the first device **106***a* can read a seed **216***a* (e.g., a generator-prime pair **7**, **11** from the user login information **121**) and create a private-public key pair that is associated with the user **202** using the first device **106***a*. In some implementations, creating the private-public key pair can include, at step **3***a*, computing **218***a* a private key (e.g., **9**) and computing a public key (e.g., **4**). In some implementations, generation of public and private keys can use generator G, prime P pair (e.g., **7**, **11**), where G<P, an example of which is described with reference to FIG. **2**F. At step **4***a*, the public key is published **220***a*, e.g., stored as the public key **214***a*. The private key n and the public key **4** constitute the private-public key pair, yet each typically is stored in a

different location. For example, the private key n can be stored locally on the first device **106***a*, e.g., in local storage **219**. The public key (e.g., **4**) can be stored in the user login information **121** as the public key **214***a*. In some implementations, the public key **214***a* can be stored in a row **222** that includes user login information for the user **202** on one or more devices (e.g., devices **106***a* and **106***b* in the current example). For example, the row **222** can serve as a directory entry associated with the user **202**. Each of the other rows can be used to store information for a different user.

Referring now to FIG. **2**B, at step **2***b*, after a login request (step **1***b*) by the user on a second different device **106***b*, a seed **216***b* (e.g., the generator-prime pair **7**, **11**) can be read (e.g., from the user login information **121**) and a second private-public key pair that is associated with the user can be created. The second private-public key pair is associated with the user **202** using the second different device **106***b*. For example, the second private-public key pair is different than the private-public key pair that is associated with the login by the user **202** on the first device **106***a*. In some implementations, creating the second private-public key pair can include, at step **3***b*, computing **218***b* a private key (e.g., m) and computing a second public key (e.g., **8**). At step **4***b*, the second public key is published **220***b*, e.g., by adding the second public key to the set of public keys stored as the public keys **214***a*. The private key m and the public key **8** constitute the second private-public key pair (e.g., <m, 8>), the values of which are different from those of the private-public key pair computed for the first device **106***a* (e.g., <n, 4>). In some implementations, the private key m can be stored locally on the second different device **106***b*, e.g., in local storage **221***b*. The public key (e.g., **8**) can be stored, for example, in user login information **121** with the public key **4** from the first device **106***a*. As a result, the directory entry stored in the row **222** (and associated with the user **202**) is updated, now including two public keys.

Referring now to FIG. **2**C, at step **5***a*, the second different device **106***b* can create a secret key **226***a* (e.g., 3) using the public key (e.g., 4) from the first device **106***a* and the second private key (e.g., private key m from local storage **221***b*). At step **6***a*, the second different device **106***b* can also associate **228***a* the second anonymous identifier (e.g., "Anonymous ID 2") with the secret key (e.g., 3). In some implementations, the association can include storing the association, e.g., in the linked anonymous identifiers **122**. For example, the linked anonymous identifiers **122** can include secret keys **230** and anonymous identifiers of the same users **232**. For example, a row **234** can include a secret key **230***a* (e.g., 3 or a hashed representation of 3) and the anonymous identifier **232***b* (e.g., "Anonymous ID 2") that corresponds to the association that occurred in step **6***a*. At a time subsequent to the publishing of the second public key (e.g., 8), and after the secret key **3** has been computed and an association stored (e.g., as a hashed representation) with the second different device **106***b*, the user may log in again at the first device **106***a*. As a result, a login request **208***c* can be received (e.g., by the login service) from the user at the first device **106***a*. For example, the login request **208***c* can be similar to the login request **208***a* described above. However, in this case, the login service, for example, can determine that a public key exists for another device associated with the user, e.g., the second different device **106**. Using the additional public key, a link or association can be made between the two devices **106***a* and **106***b* as described in further detail below. In some implementations, whenever the secret key is stored, the stored value can be a hashed version of the secret key, e.g., using a one-way hash function.

Referring now to FIG. **2**D, at step **5***b*, in response to the login request **208***c*, the first device **106***a* can create a secret key **226***b* (e.g., 3) using the public key (e.g., 8) from the second different device **106***b* and the first private key (e.g., private key n from local storage **221***a*). For example, the secret key can match the secret key computed by the second different device **106***b*. At step **6***b*, the first device **106***a* can also associate **228***b* the second anonymous identifier (e.g., Anonymous ID 2) with the secret key (e.g., 3). In some implementations, the association can include storing the association, e.g., in the linked anonymous identifiers **122**. For example, the row **234** containing the secret key **230***a* (e.g., 3) and the anonymous identifier **232***b* (e.g., "Anonymous ID 2") can be updated to also include the anonymous identifier **232***a* (e.g., "Anonymous ID 1"). As a result of storing the association, the anonymous identifiers **206***a* and **206***b*, as well as the devices **106***a* and **106***b*, are now linked. Further, the association among the user's various devices is achieved without storing any personally identifiable information associated with the user.

In some implementations, it is possible that one or more anonymous identifiers such as anonymous identifier **232***a* or anonymous identifier **232***b* can appear in multiple rows (e.g., three or more) in the linked anonymous identifiers **122**. This can be an indication, for example, that the device associated with the anonymous identifier is a shared device (e.g., at a library or an Internet café). In this example, the logins by several different users (e.g., three or more) would result in the creation of multiple rows in the anonymous identifiers **122**, each having the same anonymous identifier. In some implementations, when highly-shared devices are detected in this way, the highly-shared devices can be un-linked, or other considerations can be taken. For example, thresholds can be established, and if a cookie or other anonymous identifier appears in more than three rows, the associated can be considered a shared machine.

Referring to FIG. **2**E, at step **7**, the content management system **110** can receive a request for content **240***a* or **240***b* (e.g., a request for advertising content) from either the first device **106***a* or the second different device **106***b*. For example, the request for content **240***a* can be a request for an advertisement to fill an advertisement slot **242***a* on a web page **244***a* displayed on the first device **106***a*. In another example, the request for content **240***b* can be a request for an advertisement to fill an advertisement slot **242***b* on a web page **244***b* displayed on the second different device **106***b*. If the request for content **240***a* is from the first device **106***a*, for example, then the request for content can include the first anonymous identifier **232***a*. Otherwise, if the request for content **240***b* is from the second different device **106***b*, for example, then the request for content can include the anonymous identifier **232***b*.

Regardless of where the request for content originates, at step **8**, the content management system **110** can provide a content item (e.g., content items **246***a* or **246***b*) in response to the request and using the association that maps the user **202** to multiple devices (e.g., from the linked anonymous identifiers **122**). For example, the association can be represented by information in the row **234** that associates anonymous identifiers **232***a* and **232***b*, e.g., based on the same secret key **230***a*. Using this information, the content management system **110** can, for example, treat the requests for content as if they originate from the same user, regardless of the particular user device. In some implementations, identifying eligible content items for the request for content **240***b*, for example, can depend on content already provided to the same user **202** on the first device **106***a*. As a result, an

advertisement for California vacations, for example, that is intended for one impression per user can be shown on the first device **106***a* and not repeated again on the second different device **106***b*. In some implementations, it can be beneficial to provide the same advertisement once and only once to each of the user's multiple devices.

Devices **106***a* and **106***b* are two examples of devices that the user **202** may use. For example, the user **202** may use a third different device **106***c* (e.g., a smart phone). When the user **202** uses the third different device **106***c* to log in, for example, the user login service **120** can store a third different anonymous identifier **232** in the linked anonymous identifiers **122**. As a result, all three devices **106***a*-**106***c* can be associated with the user **202**, e.g., using the secret key **230***a*.

Similarly, other users can use the user login service **120** for logging in from multiple different devices. As a result of a second user logging into a fourth and a fifth device **106**, for example, the user login service **120** can store fourth and fifth different anonymous identifiers in the linked anonymous identifiers **122** (e.g., stored in association with the second user using a secret key **230** that is different from the secret key **230***a*).

FIG. **2**F shows example calculations of public, private and secret keys. Device A calculations **250** provide examples for computing a public key, a private key and a secret key on a first device, e.g., the first device **106***a*. Device B calculations **252** provide examples for computing a public key, a private key and a secret key on a second different device, e.g., the second different device **106***b*. Other methods can be used to determine public, private and secret keys.

In some implementations, the calculations can occur in steps, e.g., steps **254***a*-**254***e*. For example, in step **1** **254***a*, both devices A and B can exchange a prime P (e.g., 11) and a generator G (e.g., 7). In some implementations, the prime and generator can be stored in the user login information **121**, as described above. For example, a prime and a generator that is unique to a user (and the devices associated with the user) can be determined and stored at a time that one or more entries in the user login information **121** are created and stored.

In step **2** **254***b*, each device can generate its own private key, e.g., using a random number or in some other way. For example, device A's private key can be 6, and device B's private key can be 9. These private keys can be used in combination with at least the generator and prime from step **1** **254***a* to determine public and private keys in the following steps.

In step **3** **254***c*, each device can compute a public key. In some implementations, computing the public key can use a formula that includes the generator raised to the power of the device's private key, and a modulo P can be performed on the result. Using the generator, prime, and each of the devices' private keys, the resulting public keys for the devices can result in being 4 and 8, respectively.

At step **4** **254***d*, once the public keys are determined, the devices can share their public keys, e.g., by publishing the keys in the user login information **121** as described above. As a result, device A can know device B's public key (e.g., 8), and device B can know device A's public key (e.g., 4).

At step **5** **254***e*, secret keys can be computed, e.g., using a formula that raises the other device's public key to power of the current device's private key, and the result can undergo a modulo P (prime). As a result of the calculations, the secret key for the first and second devices can be 3. Once the secret key is determined, the value can be used by either device to update the row in the linked anonymous identifiers **122** with the device's anonymous identifier. This can be repeated for any other device associated with the same user that computes the secret key using its own private key and the public key from one of the other devices.

FIG. **2**G shows an example sequence of events for remarketing content to a user using linked anonymous identifiers of different requesting sources associated with the user. For example, the requesting sources can include the first device **106***a* (e.g., the user's mobile device), the second different device **106***b* (e.g., the user's personal computer), and other devices. Step **1** of the example sequence of events can be the linking of the two devices **106***a* and **106***b*. As described above with reference to FIGS. **2**A-**2**F, the two devices **106***a* and **106***b* can be linked by the content management system **110**, e.g., using linked identifier information stored in the linked anonymous identifiers **122**. Each identifier, for example, is associated with a user and a specific requesting source. The anonymous linking includes linking at least two different identifiers that are associated with two different requesting sources used by the user to access content, in this example, devices **106***a* and **106***b*. In some implementations, the linked anonymous identifiers **122** do not store user login information, account information, personal information or any other information that would make it possible to easily identify the user. While a Diffie-Hellman key exchange protocol is described herein as one possible way for anonymously linking identifiers and achieving remarketing across multiple requesting sources of the same user, other techniques can be used to anonymously link requesting sources.

At step **2** of the example sequence of events, the content management system **110**, for example, can identify **262** a user list. For example, user list **129***a* (e.g., associated with a topic **264** of cameras) can include multiple entries, each entry satisfying the topic (e.g., cameras). Each entry can also have an identifier **266** that is associated with a requesting source and can further include information about a device type **268** (e.g., a type of requesting source (e.g., mobile, non-mobile)). For example, in entry **265***a*, identifier **266***a* (e.g., AnonymousID**1**) can be associated with the first device **106***a* having a "Mobile" device type **268***a*, e.g., because a camera-related advertisement **270** has been shown to the user **202** on a web page **272***a*. In another example, identifier **266***c* (e.g., AnonymousID2) can be associated with the second different device **106***b* having a "Non-Mobile" device type **268***c*. However, identifiers **266***b* and **266***d* (e.g., AnonymousID3 and AnonymousID4, respectively) may be associated, for example, with the some other devices not shown in FIG. **2**G and may not be associated with the user **202** in any way.

Entries can be added to user lists **129**, for example, by the content management system **110**, for example, whenever content associated with a particular topic is provided to a user device. As will be seen in the examples that follow, it may be the case that entry **265***c* for identifier **266***c* and device type **268***c* is not yet present in the user list **129***a*, but may be added to the user list **129***a* as a result of remarketing that is based on linked anonymous identifiers. In some implementations, linked anonymous identifiers can be used to allow for an impression of content (e.g., the same content, related content or new content this is determined to be relevant to someone who has seen the initial content), for example, on a non-mobile device for a user who has been exposed to certain other specified content (i.e., the initial content) on a mobile device linked to the non-mobile device, e.g., using linked anonymous identifiers.

At step **3**, for example, identifiers **266** are linked **274** to other identifiers using the anonymous linking. For example, using information from the linked anonymous identifiers

122, the content management system 110 can associate identifier 266*a* with identifier 266*c* and/or other identifiers associated with the same user 202. It may be the case that one or more of the identifiers are associated with user devices of the user 202 on which camera-related content has yet to be provided.

At step 4, content is selected 276 for delivery to a user device associated with an entry in the user list based at least in part on the linking. For example, the content management system 110 can select a camera-related advertisement 271 to be shown on the user's non-mobile device, e.g., the second different device 106*b*. The camera-related advertisement 271 can be selected, for example, because of advertisement selection constraints specified by a content sponsor to remarket advertisements to a non-mobile device of a user who has already seen other (or the same) specified content on a mobile device. The camera-related advertisement 271 may or may not be the same advertisement as the camera-related advertisement 270, and may or may not have any relation to cameras per se (e.g., remarketing can be made to people interested in cameras but that which is remarketed may be unrelated to cameras).

FIG. 3A is a flowchart of an example process 300 for providing content to a user on any of multiple devices associated with the user. In some implementations, the content management system 110 and/or the user login service 120 can perform steps of the process 300 using instructions that are executed by one or more processors. FIGS. 1-2F are used to provide example structures for performing the steps of the process 300.

A first login request is received from a first device used by a user for logging into a service, the first login request being associated with a first anonymous identifier associated with the first device (302). For example, referring to FIG. 2A, the user login service 120 can receive the login request 208*a* from the first device 106*a* (e.g., a personal computer) being used by the user 202. The login request can be associated, for example, with the anonymous identifier 206*a* (e.g., "Anonymous ID 1") that is associated with the first device 106*a*.

A seed is read, and a first private-public key pair is created that is associated with the user when using the first device (304). As an example, the user login service 120 can read the seed 212*a* (e.g., generator-prime pair 7, 11) and provide the seed 212*a* to the first device 106*a*. Using the seed, the first device 106*a* can determine the private key (e.g., 9) and the public key (e.g., 4) associated with first device 106*a*.

A first private key associated with the first private-public key pair is stored locally in the first device, and a first public key is published in a directory entry associated with the user (306). The first device 106*a*, for example, can store the private key in local storage 221*a*. The first device 106*a* can also provide the public key (e.g., 4) to the user login service 120 for storage in user login information 121.

A second login request is received from a second different device used by the user, the second login request being associated with a second different anonymous identifier associated with the second different device (308). As an example, referring to FIG. 2B, the same user 202 can log into the second different device (e.g., a laptop computer). The user login service 120, for example, can receive the login request 208*b*. The login request can be associated, for example, with the anonymous identifier 206*b* (e.g., "Anonymous ID 2") that is associated with the second different device 106*b*.

Responsive to the received second login request (310), the seed is read, and a second private-public key pair is created that is associated with the user when using the second different device including a second different public key (312). As an example, the user login service 120 can read the seed 212*a* (e.g., generator-prime pair 7, 11) and provide the seed 212*a* to the second different device 106*b*. Using the seed, the second different device 106*b* can determine its private key (e.g., 6) and the public key (e.g., 8).

A second private key associated with the second private-public key pair is stored locally in the second different device, and the second public key is published in the directory entry associated with the user (314). The second different device 106*b*, for example, can store the private key in local storage 221*b*. The second different device 106*b* can also provide the public key (e.g., 8) to the user login service 120 for storage in user login information 121.

A secret key is created using the first public key (316). For example, referring to FIG. 2C, the second different device 106*b* can compute the secret key 230*a* (e.g., 3) using the public key (e.g., 4) from the first device and the second different device's own private key (e.g., 6). Device B calculations 502 shown in FIG. 2F provide example steps and formulas for computing the secret key.

The second anonymous identifier is associated with the secret key (318). For example, the second different anonymous identifier (e.g., Anonymous ID 2) can be stored with the secret key (e.g., a hashed version), e.g., in the linked anonymous identifiers 122, which is stored separately from the user login information 121.

At a time subsequent to the publishing of the second public key, a login request is received from the user when accessing the first device (320) and, responsive to the received request, the secret key is created using the second public key (322). As an example, the user 202 can log back into the first device 106*a*. The login request 208*a*, for example, can be received by the user login service 120. At this time, the first device 106*a* can also compute the secret key 3 using the first device's private key (e.g., 9) and the public key (e.g., 8) from the second different device 106*b*. Device A calculations 500 shown in FIG. 2F provide example steps and formulas for computing the secret key.

The first anonymous identifier is associated with the secret key (324). For example, the first anonymous identifier (e.g., Anonymous ID 2) can be stored with hashed version of the secret key in the linked anonymous identifiers 122. As a result, both anonymous identifiers are now linked. For example, the secret key, the first anonymous identifier, and the second different anonymous identifier are stored as an entry in a table, e.g., row 234. In some implementations, the association maps the secret key to both the first and the second different anonymous identifiers. In some implementations, one or more associations can be removed (e.g., deleted from the linked anonymous identifiers 122) after expiration of a first time period (e.g., 24 hours, 48 hours, or some other time period). In some implementations, the time period can be associated with an amount of time after which the user would have been expected to have logged out from either the first device or the second different device.

A request for content is received from either the first device including the first anonymous identifier or the second different device including the second different anonymous identifier (326). In one example, referring to FIG. 2E, the content management system 110 can receive, from the first device 106*a*, the request for content 240*a* that includes the anonymous identifier Anonymous ID 1. In another example, the content management system 110 can receive, from the second different device 106*b*, the request for content 240*b* that includes the anonymous identifier Anonymous ID 2.

Content is provided in response to the request using the association (**328**). For example, depending on which device sent the request for content **240***a* or **240***b*, the content management system **110** can provide content items **246***a* or **246***b* to either the first device **106***a* or the second different device **106***b*, respectively.

In some implementations, providing content in response to the request can further include identifying the user based on the association and providing content of interest to the user. For example, information (e.g., an interest in sports) that the user has provided in a user profile (or other information provided by and/or known about the user) can be used to select content which is likely of interest to the user.

Some implementations of the process **300** can include steps for linking additional devices, e.g., a third device and/or additional devices. For example, a login request can be received from a third different device used by the user, the login request being associated with a third different anonymous identifier associated with the third different device. A third different public-private key pair can be created, including a third public key. The third private key can be stored locally on the third different device, and the third public key can be published (e.g., in the user login information **121**). A secret key can be created using one of either the first public key or the second public key, in addition to the third different device's private key, e.g., using steps and formulas shown in FIG. **2**F. An association between the secret key, the first anonymous identifier, the second different anonymous identifier and the third different anonymous identifier can be stored, e.g., in the linked anonymous identifiers **122**. Subsequently, a request for content can be received from either the first device including the first anonymous identifier, the second different device including the second different anonymous identifier, or the third different device including the third different anonymous identifier. In response to request, content (e.g., content items **246***a* or **246***b*, or content items for the third different device) can be provided using the association.

FIG. **3**B is a flowchart of an example process **340** for providing content to a user on any of multiple linked devices associated with the user. In some implementations, the content management system **110** and/or the user login service **120** can perform steps of the process **340** using instructions that are executed by one or more processors. FIGS. **1**-**2**F are used to provide example structures for performing the steps of the process **340**.

Multiple anonymous identifiers associated with a user are linked by a service using a key exchange protocol without storing personally identifiable information associated with the user in the linking (**342**). For example, anonymous identifiers (e.g., browser cookies, or device Anonymous IDs **1** and **2**) of the first device **106***a* and the second different device **106***b*, respectively, can be linked by the user login service **120**. The linking, for example, can occur using key exchange techniques described above, including using public, private and secret key calculations shown in FIG. **2**E. In some implementations, public keys can be published on the user login service **120**, private keys can be stored on the corresponding local device, and secret keys can be stored in a third location (e.g., linked anonymous identifiers **122**). Other techniques can be used to link the devices, and more than two devices can be linked.

In some implementations, linking multiple anonymous identifiers can include receiving a login request (e.g., login requests **208***a* or **208***b*) from the user from plural different devices, determining a secret key using published public key information from another device associated with the user (where the secret key does not include any personally identifiable information associated with the user) and mapping the secret key to an anonymous identifier associated with each login request. For example, the secret key can be a secret key stored in the linked anonymous identifiers **122**, which does not include information about the user that can be traced back to the user (i.e., without having access to the information from the user login information **121**, the linked anonymous identifiers **122**, and private keys stored on the various user devices).

In some implementations, determining the secret key can include, at each device, creating a public-private key pair, publishing a public key of the public-private key pair, and using a private key of the public-private key pair and a public key of another device to compute the secret key.

Requests for content from a client device associated with the user are received at the service, where each request includes one of the anonymous identifiers (**344**). For example, referring to FIG. **2**E, the content management system **110** can receive the request for content **240***a* that includes the anonymous identifier Anonymous ID 1 corresponding to the first device **106***a*. In another example, the content management system **110** can receive the request for content **240***b* that includes the anonymous identifier Anonymous ID 2 corresponding to the second different device **106***b*.

Content associated with the user is provided that is responsive to the received requests and based on the linking (**346**). For example, the content management system **110** can provide content items **246***a* or **246***b* to either the first device **106***a* or the second different device **106***b*, respectively, depending on which device sent the request for content **240***a* or **240***b*.

FIG. **3**C is a flowchart of an example process **360** for providing content to a user on any of multiple devices linked using public-private keys. In some implementations, the content management system **110** and/or the user login service **120** can perform steps of the process **360** using instructions that are executed by one or more processors. FIGS. **1**-**2**F are used to provide example structures for performing the steps of the process **360**.

Public-private key pairs are created for a user each time the user logs into a service from a different device including publishing respective public keys of the user in a directory entry associated with the user (**362**). For example, FIGS. **2**A-**2**D show a sequence of actions that use public-private key pairs to link the first device **106***a* and the second different device **106***b*. The public keys in this example are stored in the user login information **121**.

A secret key is created by each device using a public key of another device that is stored in the directory (**364**). For example, FIGS. **2**C-**2**D show a sequence of actions that determine the secret key for each of the first device **106***a* and the second different device **106***b* using the public key of the other device.

The secret keys are associated with a plurality of anonymous identifiers, each anonymous identifier assigned to the user during a session associated with a respective different device (**366**). As an example, the secret key is stored in the linked anonymous identifiers **122**. Steps and formulas for computing the secret keys are shown in FIG. **2**E.

Content is provided that is associated with the user and based at least in part on the association (**368**). For example, depending on which device sent the request for content **240***a* or **240***b*, the content management system **110** can provide content items **246***a* or **246***b* to either the first device **106***a* or the second different device **106***b*, respectively.

FIG. **3**D is a flowchart of an example process **380** for remarketing content to a user using linked anonymous identifiers of requesting sources associated with the user. In some implementations, the content management system **110** and/or the user login service **120** can perform steps of the process **380** using instructions that are executed by one or more processors. FIGS. **1**-**2**G are referenced as example structures/interfaces associated with the steps of the process **380**. As described above, remarketing content to a user across multiple linked requesting sources may occur when permitted/enabled/selected by the user, e.g., based on settings in the user consents and privacy preferences **142**.

A plurality of identifiers associated with a user are anonymously linked (**382**). Each identifier is associated with a user and a specific requesting source. The anonymous linking includes linking at least two different identifiers that are associated with two different requesting sources used by the user to access content. For example, the identifiers that are associated with the user's requesting sources, such as mobile and non-mobile devices, can be linked anonymously, as described above with reference to FIGS. **2**A-**2**F. In some implementations, anonymously linking a user's requesting sources includes linking identifiers using a Diffie-Hellman key exchange protocol, e.g., using secret keys derived from seeds that are unique to each user. Other ways of linking a user's requesting sources can be used.

A user list is identified that is associated with a topic (**384**). The user list includes a plurality of entries, each entry satisfying the topic and having an identifier that is associated with a requesting source. Each entry further includes information about a type of requesting source. For example, a user list can be created for a topic "camera enthusiast" and each entry can be based on content that has been served or preferences (such as from a profile) for users that satisfy the topic. The content management system **110** can identify the user list **129***a* that is associated with the "cameras" topic **264**. Each of the identifiers **266** has a corresponding device type **268** (e.g., mobile or non-mobile). In some implementations, other kinds of information can exist in the user lists, such as any restrictions that the user has established for receiving content that is remarketed, e.g., that is not contained in the user consents and privacy preferences **142**.

In some implementations, a first identifier included in the user list can be associated with a non-mobile computing device, and a second identifier anonymously linked with the first identifier using the anonymous linking can be associated with a mobile device, or the other way around. In essence, a single entry in the user list can be used to link opportunities for remarketing content to a user who receives content on a plurality of different devices, including those that were unrelated to the user being including in (or qualifying for) the user list initially. Such different combinations of mobile and non-mobile entries for the same user can be used, for example, in remarketing content to a user, the remarketing occurring on the second device.

In some implementations, the process **380** can further include crediting a publisher associated with the second identifier, which may be mobile or non-mobile. For example, if remarketing occurs on the publisher's web page, then a pre-arranged amount can be paid to the publisher.

In some implementations, the user list can be used to select subsequent advertisements to be sent to a user at various ones of his/her access devices, and the process **380** can further include providing an advertisement to a user device based on an identifier that is linked to an entry in the user list. As an example, the content management system **110** can select subsequent camera-related advertisements to provide to a user based on the camera-related user list **129***a* and devices that are anonymously linked for the user.

An entry in the user list is linked to other identifiers using the anonymous linking (**386**). For example, the content management system **110** can link identifier **266***a* from entry **265***a* with other identifiers, e.g., using the linked anonymous identifiers **232***a* and **232***b* in the anonymously linked identifiers **122**. The linking in the example, can link entries **265***a* and, if it already exists in the user list **129***a*, entry **265***c*. Alternatively, entry **265***c* can be created and inserted into the user list **129***a* based on the linked anonymous identifiers **232***a* and **232***b*. In some implementations, no new entries are needed to be added to the user list as the linking provides sufficient nexus.

Content is selected for delivery to a user device associated with an entry in the user list based at least in part on the linking (**388**). For example, the content management system **110** can provide the camera-related advertisement **271** for presentation on the web page **272***b*.

In some implementations, selecting content can include selecting content for purposes of remarketing content to a user on a second one of multiple requesting sources associated with the user after presentation of the or qualifying content to the user on a first one of the multiple requesting sources associated with the user. For example, the content management system **110** can select the camera-related advertisement **271** in part because of remarketing-related selection criteria that a content sponsor has established for delivery of their content.

In some implementations, selecting content can be based at least in part on interest profiles for the user on or associated with each of the different multiple requesting sources. For example, user **202** may have a user-provided (or otherwise inferred) profile associated with the first device **106***a* that indicates an interest in cameras. The interest can then be used to select camera-related content for other requesting sources associated with the user (e.g., the second different device **106***b*).

In some implementations, the selection of content can be based, at least in part, on a bid (e.g., in an auction) associated with remarketing content to a user. In some implementations, a content sponsor's bid may be raised when content that is eligible to be provided meets certain remarketing criteria.

In some implementations, selecting content for delivery to the user device associated with the entry in the user list can further be based on a location of the user device. For example, if the user carries the second different device **106***b* (e.g., a mobile device) into a camera store, then the user's location in or near the camera store can be used, at least in part, in selecting a camera-related advertisement (e.g., in addition to remarketing).

In some implementations, the process **380** can also include receiving a request to provide a resource to a requesting source and providing to a given device associated with the requesting source an identifier upon access to the resource. For example, in response to a request for content, the content management system **110** can provide the content (e.g., a camera-related advertisement **271**) and the identifier "AnonymousID2" to the second different device **106***b*.

In some implementations, the process **380** can also include receiving a request for a third party content item wherein the request includes an identifier and determining when the identifier matches an entry in the user list including determining when the identifier matches an entry in the user list or an identifier associated with an identifier in the user list based at least in part on the anonymous linking. As an

example, when the content management system **110** receives a request for content, e.g., from the first device **106***a* for a third-party camera-related advertisement, the request can include "AnonymousID1," which the content management system **110** can use to match with other requesting resources that are anonymously linked to the first device **106***a*.

In some implementations, the process **380** can further include identifying a user device associated with linked impressions or interactions from two different requesting sources, wherein an impression has occurred on a first requesting source and an interaction has occurred on a second different requesting source and identifying content to serve to other users having similar interactions with multiple requesting sources. Identifying content, for example, can include identifying content to provide to a user device when a user whose identifier linked by the anonymous linking requests content.

Some implementations can determine an affective order of remarketing content to various types of devices. For example, some implementations of the process **380** can further include determining an effective sequence of selecting content for delivery to mobile and non-mobile devices associated with a same user. The effective sequence, for example, is associated with user behavior of a greater value to a content sponsor than user behavior associated with other different sequences of selecting content for delivery to mobile and non-mobile devices associated with a same user. Some implementations of the process **380** can further include selecting content for delivery to a user device associated with an entry in the user list based at least in part on the effective sequence. For example, it may be determined that the most effective order of delivering camera-related content in a remarketing campaign is to provide the content first to a user's non-mobile device, then remarket related content to the user's mobile device. The determination can be made, for example, if more conversions and/or other user interactions are discovered to occur using the effective sequence as compared to other sequences.

FIG. **4** is a block diagram of computing devices **400**, **450** that may be used to implement the systems and methods described in this document, as either a client or as a server or plurality of servers. Computing device **400** is intended to represent various forms of digital computers, such as laptops, desktops, workstations, personal digital assistants, servers, blade servers, mainframes, and other appropriate computers. Computing device **400** is further intended to represent any other typically non-mobile devices, such as televisions or other electronic devices with one or more processers embedded therein or attached thereto. Computing device **450** is intended to represent various forms of mobile devices, such as personal digital assistants, cellular telephones, smartphones, and other computing devices. The components shown here, their connections and relationships, and their functions, are meant to be exemplary only, and are not meant to limit implementations of the inventions described and/or claimed in this document.

Computing device **400** includes a processor **402**, memory **404**, a storage device **406**, a high-speed interface **408** connecting to memory **404** and high-speed expansion ports **410**, and a low speed interface **412** connecting to low speed bus **414** and storage device **406**. Each of the components **402**, **404**, **406**, **408**, **410**, and **412**, are interconnected using various busses, and may be mounted on a common motherboard or in other manners as appropriate. The processor **402** can process instructions for execution within the computing device **400**, including instructions stored in the memory **404** or on the storage device **406** to display graphical information for a GUI on an external input/output device, such as display **416** coupled to high speed interface **408**. In other implementations, multiple processors and/or multiple buses may be used, as appropriate, along with multiple memories and types of memory. Also, multiple computing devices **400** may be connected, with each device providing portions of the necessary operations (e.g., as a server bank, a group of blade servers, or a multi-processor system).

The memory **404** stores information within the computing device **400**. In one implementation, the memory **404** is a computer-readable medium. In one implementation, the memory **404** is a volatile memory unit or units. In another implementation, the memory **404** is a non-volatile memory unit or units.

The storage device **406** is capable of providing mass storage for the computing device **400**. In one implementation, the storage device **406** is a computer-readable medium. In various different implementations, the storage device **406** may be a floppy disk device, a hard disk device, an optical disk device, or a tape device, a flash memory or other similar solid state memory device, or an array of devices, including devices in a storage area network or other configurations. In one implementation, a computer program product is tangibly embodied in an information carrier. The computer program product contains instructions that, when executed, perform one or more methods, such as those described above. The information carrier is a computer- or machine-readable medium, such as the memory **404**, the storage device **406**, or memory on processor **402**.

The high speed controller **408** manages bandwidth-intensive operations for the computing device **400**, while the low speed controller **412** manages lower bandwidth-intensive operations. Such allocation of duties is exemplary only. In one implementation, the high-speed controller **408** is coupled to memory **404**, display **416** (e.g., through a graphics processor or accelerator), and to high-speed expansion ports **410**, which may accept various expansion cards (not shown). In the implementation, low-speed controller **412** is coupled to storage device **406** and low-speed expansion port **414**. The low-speed expansion port, which may include various communication ports (e.g., USB, Bluetooth, Ethernet, wireless Ethernet) may be coupled to one or more input/output devices, such as a keyboard, a pointing device, a scanner, or a networking device such as a switch or router, e.g., through a network adapter.

The computing device **400** may be implemented in a number of different forms, as shown in the figure. For example, it may be implemented as a standard server **420**, or multiple times in a group of such servers. It may also be implemented as part of a rack server system **424**. In addition, it may be implemented in a personal computer such as a laptop computer **422**. Alternatively, components from computing device **400** may be combined with other components in a mobile device (not shown), such as device **450**. Each of such devices may contain one or more of computing device **400**, **450**, and an entire system may be made up of multiple computing devices **400**, **450** communicating with each other.

Computing device **450** includes a processor **452**, memory **464**, an input/output device such as a display **454**, a communication interface **466**, and a transceiver **468**, among other components. The device **450** may also be provided with a storage device, such as a microdrive or other device, to provide additional storage. Each of the components **450**, **452**, **464**, **454**, **466**, and **468**, are interconnected using

various buses, and several of the components may be mounted on a common motherboard or in other manners as appropriate.

The processor **452** can process instructions for execution within the computing device **450**, including instructions stored in the memory **464**. The processor may also include separate analog and digital processors. The processor may provide, for example, for coordination of the other components of the device **450**, such as control of user interfaces, applications run by device **450**, and wireless communication by device **450**.

Processor **452** may communicate with a user through control interface **458** and display interface **456** coupled to a display **454**. The display **454** may be, for example, a TFT LCD display or an OLED display, or other appropriate display technology. The display interface **456** may comprise appropriate circuitry for driving the display **454** to present graphical and other information to a user. The control interface **458** may receive commands from a user and convert them for submission to the processor **452**. In addition, an external interface **462** may be provided in communication with processor **452**, so as to enable near area communication of device **450** with other devices. External interface **462** may provide, for example, for wired communication (e.g., via a docking procedure) or for wireless communication (e.g., via Bluetooth or other such technologies).

The memory **464** stores information within the computing device **450**. In one implementation, the memory **464** is a computer-readable medium. In one implementation, the memory **464** is a volatile memory unit or units. In another implementation, the memory **464** is a non-volatile memory unit or units. Expansion memory **474** may also be provided and connected to device **450** through expansion interface **472**, which may include, for example, a subscriber identification module (SIM) card interface. Such expansion memory **474** may provide extra storage space for device **450**, or may also store applications or other information for device **450**. Specifically, expansion memory **474** may include instructions to carry out or supplement the processes described above, and may include secure information also. Thus, for example, expansion memory **474** may be provide as a security module for device **450**, and may be programmed with instructions that permit secure use of device **450**. In addition, secure applications may be provided via the SIM cards, along with additional information, such as placing identifying information on the SIM card in a non-hackable manner.

The memory may include for example, flash memory and/or MRAM memory, as discussed below. In one implementation, a computer program product is tangibly embodied in an information carrier. The computer program product contains instructions that, when executed, perform one or more methods, such as those described above. The information carrier is a computer- or machine-readable medium, such as the memory **464**, expansion memory **474**, or memory on processor **452**.

Device **450** may communicate wirelessly through communication interface **466**, which may include digital signal processing circuitry where necessary. Communication interface **466** may provide for communications under various modes or protocols, such as GSM voice calls, SMS, EMS, or MMS messaging, CDMA, TDMA, PDC, WCDMA, CDMA2000, or GPRS, among others. Such communication may occur, for example, through radio-frequency transceiver **468**. In addition, short-range communication may occur, such as using a Bluetooth, WiFi, or other such transceiver (not shown). In addition, GPS receiver module **470** may provide additional wireless data to device **450**, which may be used as appropriate by applications running on device **450**.

Device **450** may also communicate audibly using audio codec **460**, which may receive spoken information from a user and convert it to usable digital information. Audio codec **460** may likewise generate audible sound for a user, such as through a speaker, e.g., in a handset of device **450**. Such sound may include sound from voice telephone calls, may include recorded sound (e.g., voice messages, music files, etc.) and may also include sound generated by applications operating on device **450**.

The computing device **450** may be implemented in a number of different forms, as shown in the figure. For example, it may be implemented as a cellular telephone **480**. It may also be implemented as part of a smartphone **482**, personal digital assistant, or other mobile device.

Various implementations of the systems and techniques described here can be realized in digital electronic circuitry, integrated circuitry, specially designed ASICs (application specific integrated circuits), computer hardware, firmware, software, and/or combinations thereof. These various implementations can include implementation in one or more computer programs that are executable and/or interpretable on a programmable system including at least one programmable processor, which may be special or general purpose, coupled to receive data and instructions from, and to transmit data and instructions to, a storage system, at least one input device, and at least one output device.

These computer programs (also known as programs, software, software applications or code) include machine instructions for a programmable processor, and can be implemented in a high-level procedural and/or object-oriented programming language, and/or in assembly/machine language. As used herein, the terms "machine-readable medium" "computer-readable medium" refers to any computer program product, apparatus and/or device (e.g., magnetic discs, optical disks, memory, Programmable Logic Devices (PLDs)) used to provide machine instructions and/or data to a programmable processor, including a machine-readable medium that receives machine instructions as a machine-readable signal. The term "machine-readable signal" refers to any signal used to provide machine instructions and/or data to a programmable processor.

To provide for interaction with a user, the systems and techniques described here can be implemented on a computer having a display device (e.g., a CRT (cathode ray tube) or LCD (liquid crystal display) monitor) for displaying information to the user and a keyboard and a pointing device (e.g., a mouse or a trackball) by which the user can provide input to the computer. Other kinds of devices can be used to provide for interaction with a user as well; for example, feedback provided to the user can be any form of sensory feedback (e.g., visual feedback, auditory feedback, or tactile feedback); and input from the user can be received in any form, including acoustic, speech, or tactile input.

The systems and techniques described here can be implemented in a computing system that includes a back end component (e.g., as a data server), or that includes a middleware component (e.g., an application server), or that includes a front end component (e.g., a client computer having a graphical user interface or a Web browser through which a user can interact with an implementation of the systems and techniques described here), or any combination of such back end, middleware, or front end components. The components of the system can be interconnected by any

form or medium of digital data communication (e.g., a communication network). Examples of communication networks include a local area network ("LAN"), a wide area network ("WAN"), and the Internet.

The computing system can include clients and servers. A client and server are generally remote from each other and typically interact through a communication network. The relationship of client and server arises by virtue of computer programs running on the respective computers and having a client-server relationship to each other.

While this specification contains many specific implementation details, these should not be construed as limitations on the scope of any inventions or of what may be claimed, but rather as descriptions of features specific to particular implementations of particular inventions. Certain features that are described in this specification in the context of separate implementations can also be implemented in combination in a single implementation. Conversely, various features that are described in the context of a single implementation can also be implemented in multiple implementations separately or in any suitable subcombination. Moreover, although features may be described above as acting in certain combinations and even initially claimed as such, one or more features from a claimed combination can in some cases be excised from the combination, and the claimed combination may be directed to a subcombination or variation of a subcombination.

Similarly, while operations are depicted in the drawings in a particular order, this should not be understood as requiring that such operations be performed in the particular order shown or in sequential order, or that all illustrated operations be performed, to achieve desirable results. In certain circumstances, multitasking and parallel processing may be advantageous. Moreover, the separation of various system components in the implementations described above should not be understood as requiring such separation in all implementations, and it should be understood that the described program components and systems can generally be integrated together in a single software product or packaged into multiple software products.

Thus, particular implementations of the subject matter have been described. Other implementations are within the scope of the following claims. In some cases, the actions recited in the claims can be performed in a different order and still achieve desirable results. In addition, the processes depicted in the accompanying figures do not necessarily require the particular order shown, or sequential order, to achieve desirable results. In certain implementations, multitasking and parallel processing may be advantageous.

What is claimed is:

1. A computer-implemented method comprising:

anonymously linking, by one or more servers, a plurality of identifiers, including linking at least two different identifiers that are associated with two different requesting devices used by a same user to access content;

identifying, by one or more servers, a user list associated with a topic, wherein the user list includes a separate entry for each different user that has been determined to satisfy the topic and having an identifier that is associated with a requesting device and further including information about a type of requesting device;

updating, by the one or more servers, the user list including linking a single user identifier entry for the same user to other identifiers that have been assigned to the same user but are not included in the list, wherein the linking is based on the anonymous linking;

receiving a content request from a user and associated user device;

analyzing the user list including:

determining that the content request is associated with a given user identifier that is not included in the user list; and

determining that the given user identifier associated with the request is linked to the single user identifier entry that is included in the user list based on the linking; and

selecting, based on the determination that the given user identifier is linked to the single user identifier entry that is included in the user list, content for delivery to the user device associated with the request based at least in part on the topic associated with the user list even though the given user identifier is not included in the user list.

2. The method of claim **1** wherein selecting content includes selecting content for purposes of remarketing content to a user on a second one of multiple requesting devices associated with the user after presentation of content to the user on a first one of the multiple requesting devices associated with the user.

3. The method of claim **2** wherein selecting content is based at least in part on interest profiles for the user on each of the different multiple requesting devices.

4. The method of claim **1** further comprising:

receiving a request to provide a resource to a requesting device; and

providing to a given device associated with the requesting device an identifier upon access to the resource.

5. The method of claim **1** further comprising:

receiving a request for a third party content item wherein the request includes an identifier; and

determining when the identifier matches an entry in the user list including determining when the identifier matches an entry in the user list or an identifier associated with an identifier in the user list based at least in part on the anonymous linking.

6. The method of claim **1** wherein a first identifier included in the user list is associated with a non-mobile computing device and a second identifier anonymously linked with the first identifier using the anonymous linking is associated with a mobile device.

7. The method of claim **1** wherein a first identifier included in the user list is associated with a mobile computing device and a second identifier anonymously linked with the first identifier using the anonymous linking is associated with a non-mobile device.

8. The method of claim **6** or **7** further comprising:

crediting a publisher associated with the second identifier.

9. The method of claim **1** wherein the user list is used to select subsequent advertisements to be sent to a user device, and wherein the method further comprises providing an advertisement to a user device based on an identifier that is linked to an entry in the user list.

10. The method of claim **1** wherein the different requesting devices are selected from the group comprising: a mobile device including a smart phone, a laptop computer, a tablet, a desktop device, a set-top box, a television, a browser, an application on a mobile device, or a stand-alone application.

11. The method of claim **1** further comprising:

identifying a user device associated with linked impressions or interactions from two different requesting devices, wherein an impression has occurred on a first

requesting device and an interaction has occurred on a second different requesting device; and

identifying content to serve to other users having similar interactions with multiple requesting devices.

12. The method of claim **9** wherein identifying content includes identifying content to provide to a user device when a user whose identifier linked by the anonymous linking requests content.

13. The method of claim **1** wherein anonymously linking includes linking identifiers using a Diffie-Hellman key exchange protocol.

14. The method of claim **1** wherein anonymously linking includes linking identifiers using a secret key derived from a seed that is unique to the user.

15. The method of claim **1** wherein selecting content for delivery to the user device associated with the entry in the user list is further based on a location of the user device.

16. The method of claim **1** further comprising:

determining an effective sequence of selecting content for delivery to mobile and non-mobile devices associated with a same user, the effective sequence associated with user behavior of a greater value to a content sponsor than user behavior associated with other different sequences of selecting content for delivery to mobile and non-mobile devices associated with a same user; and

selecting content for delivery to a user device associated with an entry in the user list based at least in part on the effective sequence.

17. A non-transitory computer program product embodied in a tangible medium including instructions, that when executed, cause a processor to:

anonymously link, by one or more servers, a plurality of identifiers, including linking at least two different identifiers that are associated with two different requesting devices used by a same user to access content;

identify, by one or more servers, a user list associated with a topic, wherein the user list includes a separate entry for each different user that has been determined to satisfy the topic and having an identifier that is associated with a requesting device and further including information about a type of requesting device;

update, by the one or more servers, the user list including linking a single user identifier entry for the same user to other identifiers that have been assigned to the same user but are not included in the list, wherein the linking is based on the anonymous linking;

receive a content request from a user and associated user device;

analyze the user list including:

determining that the content request is associated with a user identifier that is not included in the user list; and;

determining that the given user identifier associated with the request is linked to the single user identifier entry that is included in the user list based on the linking; and

select, based on the determination that the given user identifier is linked to the single user identifier entry that is included in the user list, content for delivery to the user device associated with the request based at least in part on the topic associated with the user list even though the given user identifier is not included in the user list.

18. The computer program product of claim **17** wherein selecting content includes selecting content for purposes of remarketing content to a user on a second one of multiple requesting devices associated with the user after presentation of content to the user on a first one of the multiple requesting devices associated with the user, and wherein selecting content is based at least in part on interest profiles for the user on each of the different multiple requesting devices.

19. A system comprising:

a processor; and

a memory including instructions that when executed cause the processor to:

anonymously link, by one or more servers, a plurality of identifiers, including linking at least two different identifiers that are associated with two different requesting devices used by a same user to access content;

identify, by one or more servers, a user list associated with a topic, wherein the user list includes a separate entry for each different user that has been determined to satisfy the topic and having an identifier that is associated with a requesting device and further including information about a type of requesting device;

update, by the one or more servers, the user list including linking a single user identifier entry for the same user to other identifiers that have been assigned to the same user but are not included in the list, wherein the linking is based on the anonymous linking;

receive a content request from a user and associated user device;

analyze the user list including:

determining that the content request is associated with a user identifier that is not included in the user list; and

determining that the given user identifier associated with the request is linked to the single user identifier entry that is included in the user list based on the linking; and

select, based on the determination that the given user identifier is linked to the single user identifier entry that is included in the user list, content for delivery to the user device associated with the request based at least in part on the topic associated with the user list even though the given user identifier is not included in the user list.

20. The system of claim **19** wherein selecting content includes selecting content for purposes of remarketing content to a user on a second one of multiple requesting devices associated with the user after presentation of content to the user on a first one of the multiple requesting devices associated with the user, and wherein selecting content is based at least in part on interest profiles for the user on each of the different multiple requesting devices.

* * * * *

UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

PATENT NO. : 9,514,446 B1
APPLICATION NO. : 13/648651
DATED : December 6, 2016
INVENTOR(S) : Rajkumar et al.

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

On the Title Page:

The first or sole Notice should read --

Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 519 days.

Signed and Sealed this
Twenty-fifth Day of September, 2018

Andrei Iancu
Director of the United States Patent and Trademark Office